MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi dell'art. 6, comma 1, lett. a) del d.lgs. 8 giugno 2001, n. 231

REV.	PUNTI OGGETTO DELLA REVISIONE	data
1.0	Prima revisione	16/09/2016
2.0	Aggiornamento reati presupposto, Whistleblowing e altre integrazion minori	20/03/2020
3.0	Aggiornamento normativo reati presupposto e nuova governance societaria	05/10/2020

Ottobre 2020

Sommario

PARTE GENERALE

Il Decreto Legislativo 231/2001

Premessa

La società Philogen Spa e le Società da essa controllate (di seguito "Gruppo" o "Philogen") sono sensibili all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione e immagine, delle aspettative dei propri azionisti e del lavoro dei propri dipendenti.
Philogen ha ritenuto conforme alla propria politica procedere all'attuazione del Modello di organizzazione, gestione e controllo (di seguito "Modello Organizzativo" o "Modello") previsto dal Decreto Legislativo 231/2001 (di seguito anche "Decreto").
A tal fine, Philogen ha avviato negli ultimi mesi dell'anno 2010 un progetto di analisi dei propri strumenti organizzativi, di gestione e di controllo, volto a verificare la corrispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto. Preliminarmente, con delibera del C.d.A. di data 25 novembre 2010, Philogen ha approvato il Codice Etico;
Di seguito, sempre con delibera del C.d.A. del 21 dicembre 2010, Philogen ha adottato il Modello organizzativo previsto dal D.lgs. 231/2001 unitamente ai suoi allegati, contestualmente, veniva nominato l'Organo monocratico di Vigilanza nella persona del Dott. Marco Tanini.
Successivamente, alla riunione del C.d.A. del 27 gennaio 2012, veniva approvata la versione rivista del Modello organizzativo (dicembre 2011).
A seguito di necessari aggiornamenti dovuti all'evoluzione normativa, con delibera del C.d.A., di data 22 novembre 2012 veniva adottata una nuova versione del Modello stesso (novembre 2012).
In data 26 giugno 2013 il C.d.A. prendeva atto dell'entrata in vigore dell'art. 25 duodecies del Decreto e delle importanti modifiche apportate dalla cd. "Legge Anticorruzione" (L. n. 190/12), inoltre, in considerazione del fatto che la quotazione in Borsa non era stata a suo tempo completata, rilevava i numerosi cambiamenti sia in ordine ai reati presupposto, sia le numerose procedure interne, ormai superflue ed evidenziava quindi la necessità di rivedere sostanzialmente il *risk assessment* e quindi l'intero modello semplificandone gli aspetti ormai ridondanti e aggiornandone il contenuto. Veniva quindi confermato il mandato agli incaricati di rivedere integralmente l'elaborato.
Nelle more della revisione integrale del Modello, con il D.L. 93 del 14 agosto 2013 sulla violenza di genere, venivano introdotti i reati presupposto di frode informatica e di contraffazione di carte di credito, nonché i delitti sulla privacy. La legge n.119 del 15/10/2013 di conversione del decreto eliminava detto ampliamento. Si arrivava quindi all'elaborazione del modello e conseguente approvazione da parte del C.d.A. in data 23 ottobre 2013.
In seguito, la L. n. 186/2014 ha inserito all'art. 648-ter.1 del codice penale il nuovo reato di auto riciclaggio, parte anch'esso, dell'elenco dei reati presupposto della responsabilità amministrativa degli Enti mentre le Leggi n. 68 e n. 69 del 2015 hanno apportato importanti modifiche e integrazioni sotto il profilo dei reati ambientali e societari.

Stante l'entrata in vigore della suindicata normativa, e le intervenute modifiche all'assetto e alla Governance societaria, si è reso quindi improrogabile l'aggiornamento del Modello.
Questo Modello e i principi in esso contenuti si applicano a tutti gli Amministratori, ai Sindaci, ai Soggetti che operano per la Società incaricata della Revisione dell'Azienda (più avanti indicati come 'Amministratori', 'Sindaci' e 'Revisore'), ai Dipendenti, inclusi i Dirigenti (di seguito, congiuntamente indicati quali 'Personale'), senza eccezione alcuna, nonché a tutti coloro che, seppur esterni alla Società stessa, operino, direttamente o indirettamente, per Philogen (ad es., procuratori, agenti, collaboratori a qualsiasi titolo, consulenti, fornitori, partner commerciali, di seguito, indicati quali 'Terzi Destinatari'). Tutti i soggetti indicati nel presente paragrafo saranno complessivamente definiti, nel proseguo, 'Destinatari' o, singolarmente, 'Destinatario'.

Normativa

Il Decreto Legislativo 8 giugno 2001, n. 231, *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della Legge 29 settembre 2000, n. 300"* ha introdotto per la prima volta nel nostro ordinamento la responsabilità in sede penale degli Enti, che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito[1].

L'ampliamento della responsabilità mira a coinvolgere nella punizione di taluni illeciti penali il patrimonio degli Enti stessi e, in definitiva, gli interessi economici dei Soci, i quali, fino all'entrata in vigore della legge in esame, non subivano conseguenze dalla realizzazione di reati commessi, con vantaggio della Società, da Amministratori e/o Dipendenti. Il principio di personalità della responsabilità penale li lasciava, infatti, indenni da conseguenze sanzionatorie, diverse dall'eventuale risarcimento del danno, se e in quanto esistente.

Sul piano delle conseguenze penali, infatti, soltanto gli artt. 196 e 197 c.p. prevedevano (e prevedono tuttora) un'obbligazione civile delle persone giuridiche per il pagamento di multe o ammende inflitte, ma solo in caso d'insolvibilità dell'autore materiale del fatto.
L'innovazione normativa non è di poco conto, in quanto né l'Ente, né i Soci delle Società o Associazioni possono dirsi estranei al procedimento penale per reati commessi a vantaggio o nell'interesse dell'Ente. Ciò, ovviamente, determina un interesse di quei soggetti (Soci, Associati, ecc.) che partecipano alle vicende patrimoniali dell'Ente, al controllo della regolarità e della legalità dell'operato sociale.

[1] La previsione di una responsabilità amministrativa (ma di fatto penale) degli enti per determinate fattispecie di reato era contenuta nell'art. 2 della Convenzione OCSE del 17 dicembre 1997 sulla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali. Tale tipo di responsabilità è stato successivamente introdotto nel nostro ordinamento dall'art. 11 della legge 29 settembre 2000, n. 300, di ratifica ed esecuzione delle convenzioni OCSE e Unione Europea contro la corruzione nel commercio internazionale e contro la frode ai danni della Comunità Europea.
L'art. 11, in particolare, delegava il Governo a disciplinare l'articolazione di questo tipo di responsabilità. In attuazione di tale delega, il Governo ha adottato il d. lgs. n. 231/2001.

L'evoluzione dei reati

Quanto alla tipologia di reati cui si applica la disciplina in esame, il legislatore delegato ha operato una scelta minimalista rispetto alle indicazioni contenute nella Legge delega (L. n. 300/2000). Infatti, delle quattro categorie di reati ivi indicate il Governo ha preso in considerazione soltanto quelle previste dagli **artt. 24** (*Indebita percezione di erogazioni pubbliche, Truffa in danno dello Stato o di altro ente pubblico o per il conseguimento di erogazioni pubbliche e Frode informatica in danno dello Stato o di altro ente pubblico)* e **25** (*Concussione e Corruzione*), evidenziando, nella relazione di accompagnamento al D.lgs. n. 231/2001, la prevedibile estensione della disciplina in questione anche ad altre categorie di reati. Tale relazione è stata profetica, giacché successivi interventi normativi hanno ampiamente esteso il catalogo dei reati cui si applica la disciplina del Decreto n. 231/2001.

Infatti la Legge 23 novembre 2001, n. 409[2] di conversione del D.L. n. 350/2001 recante disposizioni urgenti in vista dell'euro, ha introdotto, all'art. 4, un nuovo articolo al Decreto n. 231 (**art. 25-*bis*)** relativo alle falsità in monete, carte di pubblico credito e in valori di bollo.

L'intervento più importante è rappresentato però dal D. Lgs. n. 61/2002 in tema di reati societari[3], che ha aggiunto al Decreto n. 231 l'**art. 25-*ter***, estendendo la responsabilità amministrativa ad alcune fattispecie di reati societari commessi nell'interesse (ma non anche a vantaggio, come invece previsto dal decreto n. 231) della società da Amministratori, Direttori Generali, Liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si fosse realizzato se essi avessero vigilato in conformità agli obblighi inerenti alla loro carica. L'art. 25-*ter* disciplina, in particolare, i reati di falsità in bilancio, nelle relazioni e nelle altre comunicazioni sociali, falso in prospetto[4], falsità nelle relazioni o comunicazioni della società di revisione, impedito controllo, formazione fittizia del capitale, indebita restituzione dei conferimenti, illegale ripartizione degli utili e delle riserve, illecite operazioni sulle azioni o quote sociali o della società controllante, operazioni in pregiudizio dei creditori, indebita ripartizione dei beni sociali da parte dei liquidatori, indebita influenza sull'assemblea, aggiotaggio, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza.

Successivamente, la Legge di *"Ratifica ed esecuzione della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999"*[5]

---

[2] Legge n. 409/2001 pubblicata nella Gazzetta Ufficiale n. 274 del 24 novembre 2001.

[3] Il decreto legislativo n. 61/2002 sulla disciplina degli illeciti penali ed amministrativi riguardanti le società commerciali. Il decreto è stato pubblicato l'11 aprile 2002 sulla Gazzetta Ufficiale - Serie Generale n. 88 del 15 aprile 2002. Con questo provvedimento il Governo ha dato attuazione all'art. 11 della legge delega sulla riforma del diritto societario (l. n.366/2001), approvata il 3 ottobre 2001. Le norme menzionate sono state successivamente modificate con la l. n.262/2005 citata nel seguito.

[4] L'art. 2623 c.c. che disciplinava il reato di falso in prospetto è stato abrogato e sostituito con l'art. 173-bis TUF.
Nonostante tale modifica, il richiamo all'art. 2623 contenuto nell'art. 25-ter del d.lgs. n. 231/2001 non è stato sostituito con il richiamo all'art. 173-*bis* TUF, ciò che dovrebbe comportare l'inapplicabilità del decreto 231 al reato di falso in prospetto.

[5] Legge n. 7/2003, in G.U. n. 21 del 27 gennaio 2003.

ha inserito un nuovo **art. 25-*quater*** al Decreto 231, che stabilisce la responsabilità amministrativa dell'Ente anche riguardo alla commissione dei delitti aventi finalità di terrorismo o di eversione dell'ordine democratico. La Legge trova inoltre applicazione (art. 25-*quater*, ult. co.) con riferimento alla commissione di delitti, diversi da quelli espressamente richiamati, *"che siano comunque stati posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999*".

La Legge contenente *"Misure contro la tratta delle persone"*[6] ha, poi, introdotto un nuovo articolo al Decreto, il **25-*quinquies***, che estende il regime della responsabilità amministrativa dell'Ente anche in relazione alla commissione dei delitti contro la personalità individuale disciplinati dalla sezione I del capo III del titolo XII del libro II del codice penale.

Successivi interventi diretti a modificare la disciplina della responsabilità amministrativa degli Enti sono stati attuati con la Legge Comunitaria per il 2004[7] (art. 9) che, tra l'altro, ha recepito mediante norme d'immediata applicazione la Direttiva 2003/6/CE del Parlamento europeo e del Consiglio, del 28 gennaio 2003, relativa all'abuso d'informazioni privilegiate e alla manipolazione del mercato (c.d. abusi di mercato), e con la legge *"Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari"*, che ha apportato alcune modifiche al regime della responsabilità amministrativa delle persone giuridiche con riguardo ad alcuni reati societari[8].

La nuova normativa in materia di abusi di mercato ha ampliato l'ambito di applicazione del Decreto 231, facendo rientrare nel novero degli illeciti "presupposto" della responsabilità amministrativa degli Enti le fattispecie dell'abuso d'informazioni privilegiate (c.d. insider trading) e della manipolazione del mercato.

La Legge Comunitaria 2004, in particolare, è intervenuta sia sul codice civile, sia sul Testo Unico della Finanza (TUF).

Quanto al codice civile è stato modificato l'art. 2637, che sanzionava il reato di aggiotaggio commesso su strumenti finanziari, sia quotati sia non quotati. La norma si applica adesso ai soli casi di aggiotaggio posti in essere con riferimento a strumenti finanziari non quotati o per i quali non è stata presentata richiesta di ammissione alle negoziazioni in un mercato regolamentato, e non invece a quelli quotati, cui si applicano le norme del TUF in materia di manipolazione di mercato. È invece riferita alle sole informazioni privilegiate relative a

---

[6] Legge 11 agosto 2003, n. 228, recante *"Misure contro la tratta di persone"*. Il provvedimento è stato pubblicato nella Gazzetta Ufficiale 23 agosto 2003, n. 195.

[7] Legge 18 aprile 2005, n. 62, contenente *"Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2004".* Il provvedimento è stato pubblicato nella Gazzetta Ufficiale n.96 del 27 aprile 2005 - Supplemento ordinario n.76.

[8] Legge 28 dicembre 2005, n. 262 recante "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari", pubblicata nella Gazzetta Ufficiale n. 301 del 28 dicembre 2005 - Supplemento Ordinario n. 208.

società emittenti disciplinate dal TUF la nuova fattispecie dell'insider trading (o abuso d'informazioni privilegiate).

La Legge n. 262/2005 sulla tutela del risparmio ha invece esteso la responsabilità degli Enti alla nuova fattispecie di reato di omessa comunicazione del conflitto d'interessi degli Amministratori, riguardante esclusivamente le società quotate, e modificato le norme sulle false comunicazioni sociali e sul falso in prospetto.

Ulteriori modifiche legislative in materia di responsabilità degli Enti sono state introdotte dalla Legge n. 7/2006[9] che vieta e punisce le c.d. pratiche d'infibulazione, dalla Legge n.38/2006[10] contenente "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet" e, infine, dalla Legge di ratifica ed esecuzione della Convenzione di Palermo sulla criminalità organizzata transnazionale del15 novembre 2000[11].
La Legge 6 febbraio 2006, n. 38, ha modificato l'ambito di applicazione dei delitti di pornografia minorile e detenzione di materiale pornografico (rispettivamente, artt. 600-ter e 600-quater c.p.), per i quali era già prevista la responsabilità dell'Ente ex Decreto 231, includendo anche le ipotesi in cui il materiale pornografico utilizzato rappresenti immagini virtuali di minori (c.d. "pedopornografia virtuale").
A sua volta la Legge n. 146/2006 di ratifica ed esecuzione della Convenzione ONU contro il crimine organizzato transnazionale, ha stabilito l'applicazione del Decreto 231 ai reati di criminalità organizzata transnazionale. Le nuove disposizioni hanno previsto la responsabilità degli Enti per gli illeciti amministrativi dipendenti dai delitti di associazione a delinquere, riciclaggio e impiego di denaro e beni di provenienza illecita, traffico di migranti e intralcio alla giustizia[12].
Successivamente, la Legge 3 agosto 2007, n. 123, con l'introduzione dell'art. **25-septies** nell'impianto normativo del D.lgs. n. 231/2001, ha ulteriormente esteso l'ambito applicativo della responsabilità amministrativa degli Enti ai reati di omicidio colposo e lesioni colpose gravi o gravissime che si verifichino in connessione alla violazione delle norme per la prevenzione degli infortuni sul lavoro o relative alla tutela dell'igiene e della salute sul lavoro[13].

Con Decreto Legislativo 21 novembre 2007, n. 231, il legislatore ha dato attuazione alla direttiva 2005/60/CE del Parlamento e del Consiglio, del 26 ottobre 2005, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività

---

9 Legge 9 gennaio 2006, n. 7, recante *"Disposizioni concernenti la prevenzione e il divieto delle pratiche di mutilazione genitale femminile"*, pubblicata nella Gazzetta Ufficiale n. 14 del 18 gennaio 2006.

10 Legge 6 febbraio 2006, n. 38, contenente *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, pubblicata nella Gazzetta Ufficiale n. 38 del 15 febbraio 2006.

11 Legge 16 marzo 2006, n. 146, recante *"Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001"*, pubblicata nella Gazzetta Ufficiale dell'11 aprile 2006, n. 85 – Suppl. Ord. n. 91.

12 La previsione relativa ai reati di riciclaggio e impiego di denaro e beni di provenienza illecita aventi carattere di transnazionalità è stata successivamente abrogata dal d.lgs. n. 231 del 21 novembre 2007.

13 Legge 3 agosto 2007, n. 123, recante *"Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa in materia"*, pubblicata in G.U. 10 agosto 2007, n. 185.

criminose e di finanziamento del terrorismo (c.d. III Direttiva antiriciclaggio)[14]. Ne consegue che l'Ente sarà ora punibile per i reati di ricettazione, riciclaggio e impiego di capitali illeciti, anche se compiuti in ambito prettamente "nazionale", sempre che ne derivi un interesse o vantaggio per l'Ente medesimo.

Attraverso la Legge n. 48 del 18 marzo 2008[15] è stata data esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001. Con l'art. 7 del testo definitivamente approvato dal Parlamento è stato aggiornato il D.lgs. 231/2001 introducendo l'art. **24-bis**, disciplinante la responsabilità amministrativa degli Enti per i Reati informatici posti in essere da soggetti che si trovino in posizione apicale o dipendente nell'interesse o a vantaggio dell'ente stesso. Tale articolo è stato poi recentemente aggiornato con l'introduzione del reato di "ostacolo alle funzioni di vigilanza ed ispezione della Presidenza del Consiglio dei Ministri in tema di sicurezza nazionale cibernetica", introdotto nel nostro ordinamento dall'art. 11 del D.L. 105/2019 convertito con modificazioni in L. 133/2019, Oltre alle sanzioni pecuniarie, l'art. 24-bis prevede la possibilità di comminare all'ente le sanzioni interdittive descritte dall'art. 9[16].

L´art. **24 ter** del D. Lgs. 231/2001, inserito dalla Legge 15 luglio 2009, n. 94, e rubricato "delitti di criminalità organizzata" prevede fra i "reati presupposto" l´associazione a delinquere "semplice" ai sensi dell´art. 416 c.p.: per la configurazione di tale fattispecie di reato è, come noto, necessaria l´associazione di tre o più persone, allo scopo di commettere più delitti.

La norma non rappresenta una novità assoluta, atteso che l´art. 416 c.p. era già da tempo previsto fra i "presupposto" (Legge 146/2006).

Tuttavia l´art. 3 della stessa L. 146/2006 ne limitava estremamente la portata, prevedendo che l´associazione a delinquere poteva comportare la responsabilità amministrativa

---

[14] Il d.lgs. n. 231/2007, recante *"Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione*", è stato pubblicato nella G.U. n. 290 del 14 dicembre 2007 - Suppl. Ordinario n. 268. Il testo è in vigore dal 29 dicembre 2007.

[15] Legge 18 marzo 2008, n. 48 recante "Ratifica *ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno", pubblicato nella G.U. 4 aprile 2008, n. 80.*

[16] In particolare si prevede che nell'ipotesi di condanna dell'ente a seguito della commissione del Reato – di accesso abusivo a sistema informatico o telematico (615-ter c.p.), d'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617-quater c.p.), di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (617-quinquies c.p.), di danneggiamento d'informazioni, dati e programmi informatici (635-bis c.p.), d'informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (635-ter c.p.), di danneggiamento di sistemi informatici o telematici (635-quater c.p.) e di sistemi informatici o telematici di pubblica utilità (635-quinquies c.p.) - saranno applicabili le sanzioni dell'interdizione dall'esercizio dell'attività, della sospensione o della revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e, infine, del divieto di pubblicizzare beni o servizi.

Si applicheranno, invece, le sanzioni interdittive dell'interdizione dall'esercizio dell'attività, della sospensione o della revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito in caso di commissione del Reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615-quater c.p.) e di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (615-quinquies c.p.).

Infine per i Reati previsti dal terzo comma dell'art. 24-bis applicheranno le sanzioni interdittive del divieto di contrattare con la pubblica amministrazione (salvo che per ottenere le prestazioni di un servizio pubblico); l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi e, ancora, il divieto di pubblicizzare beni o servizi.

dell´Ente se venivano soddisfatti i criteri di "trasnazionalità" e se il reato veniva commesso con il necessario coinvolgimento di un *gruppo criminale organizzato*[17].
E´ di tutta evidenza che tale qualificazione circoscrive notevolmente le oggettive possibilità d'integrazione del reato in questione a ipotesi "di nicchia" (territoriali o di settore economico). Da gestire, quindi, in sede di modello organizzativo, in situazioni ordinarie, con un semplice richiamo al Codice Etico o, al più, con semplici punti di controllo e, naturalmente, solo per quegli Enti che effettuano operazioni a livello internazionale.
La previsione dell´associazione a delinquere semplice, di cui all´art. 24 ter D.lgs. 231, non richiede invece tali qualificazioni.
L´impatto di tale novità legislativa appare di particolare significato: potenzialmente, ora, qualsiasi delitto dell´ordinamento giuridico italiano commesso a interesse e vantaggio dell´Ente, con il vincolo associativo dell'art. 416 c.p. potrebbe in ipotesi configurare la responsabilità "231" per la società.

La Legge comunitaria 2009, approvata definitivamente in Senato il 12 maggio, interviene sul Decreto Legislativo 231/2001 con l'approvazione di diversi provvedimenti di rango sovranazionale che spaziano dalle direttive alle decisioni quadro.
Con l'approvazione dell'articolo 19 si prevede la responsabilità in sede penale di Enti, Società, Cooperative, ecc. per i delitti ambientali (direttiva 2008/99) e per quelli relativi all'inquinamento provocato dalle navi. La Direttiva è entrata in vigore il ventesimo giorno successivo alla pubblicazione ed è stata recepita dal nostro stato.
Infatti con **l'art. 25 undecies** del d.lgs. 231/01 è stato ampliato il novero dei reati amministrativi ai reati ambientali.
Successivamente, in data 9 agosto 2012 è entrato in vigore l'art. **25 duodecies** "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare", che inserisce tra i reati presupposto anche quello dell'Impiego di cittadini di paesi terzi il cui soggiorno è irregolare, successivamente integrato con l'inclusione del reato di "caporalato" collegato all'impiego di tali soggetti clandestini sul territorio nazionale
Con la Legge n. 190 del 6.11.2012, "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" cd. "Legge Anticorruzione", pubblicata nella Gazzetta Ufficiale del 13.11.2012, il Legislatore italiano ha inteso adeguare la normativa nazionale ai dettami della Convenzione di Strasburgo del 27 gennaio 1999, ratificata con Legge n. 110 del 28.6.2012, ed ha così voluto novellare la disciplina del codice penale quanto ai reati di concussione e corruzione, modificare l'art. 2635 c.c. in tema di corruzione tra privati e introdurre nuovi reati presupposto della responsabilità amministrativa ex D.Lgs. 231/01 (L. 190/12 art. 1 co. 75 e ss.).

[17] "Legge 16 marzo 2006 n. 146, Art. 3 Definizione di reato transnazionale. Ai fini della presente legge si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:
a) sia commesso in più di uno Stato;
b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato"

In seguito la L. n. 186/2014 ha inserito all'art. 648-ter.1 del codice penale il nuovo reato di autoriciclaggio anch'esso facente parte dell'elenco dei reati presupposto della responsabilità amministrativa degli Enti ai sensi del D.L.gs 231/2001 (**art. 25 octies**).
La L. n. 68/2015, prevedendo un nuovo titolo, del Codice Penale, cioè il VI – bis intitolato "Dei delitti contro l'Ambiente", ha modificato in modo significativo il D.lgs. n. 152/06 apportando un'importante modifica e integrazione dell'**art. 25-undecies** del Decreto che ci occupa.
La successiva L. n. 69/2015 ha a sua volta introdotto alcune modifiche alla responsabilità amministrativa degli Enti sotto il profilo dei reati societari e quindi all'**art. 25–ter** del Decreto.
La Legge 167/2017 ha introdotto anche il reato di "razzismo e xenofobia" fra quelli presupposto (**art. 25-terdecies**), mentre con la la Legge n. 179/2017 è stato introdotto il principio del **whistleblowing**, ovvero un sistema di tutela dei dipendenti che scoprono la commissione di fatti illeciti (reati penali, violazioni del codice etico, del regolamento aziendale, dei codici disciplinari interni, dello Statuto dei lavoratori, episodi di corruzione sia attiva che passiva e così via) nello svolgimento della propria attività lavorativa, segnalandolo alla direzione. Tale norma ha introdotto all'art. 6 del D. 231/2001 l'obbligo di predisporre uno o piu' canali che consentano ai dipendenti, di presentare, a tutela dell'integrita' dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali dovranno garantire la riservatezza dell'identita' del segnalante nelle attivita' di gestione della segnalazione; dovrà inoltre essere garantito il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione e la previsione di sanzioni nei confronti di chi viola le misure di tutela del segnalante nonche' di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.
Gli ultimi interventi sono stati quelli della Legge 39/2019, che ha ampliato la responsabilità anche ai reati di "frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati" con l'introduzione **dell'art. 25-quaterdecies**, ed infine, quelli Decreto Legge 124/2019, convertito con modifiche nella Legge 157/2019, dove sono stati inseriti come reati presupposto anche i principali reati tributari previsti dal nostro ordinamento (false fatturazioni, dichiarazione fraudolenta), inseriti nel nuovo **art. 25 quinquiesdecies**.

I reati

Alla data della revisione del presente documento i reati previsti dal D.lgs. 231/01 riguardano le seguenti tipologie:

Reati commessi nei rapporti con la Pubblica Amministrazione (art. 24, d.lgs. 231/01).

- Malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis c.p.);

- Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico o delle Comunità europee (art.316-ter c.p.);
- Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art.640, comma 2, n.1, c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.).

Delitti informatici e trattamento illecito di dati (art. 24-bis, d.lgs. 231/01) .

- Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.);
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- 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.);
- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
  Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
- Ostacolo alle funzioni ispettive e di vigilanza della Presidenza del Consiglio dei ministri in tema di sicurezza nazionale cibernetica (art. 11 L. 133/2019).

Delitti di criminalità organizzata (art. 24-ter, d.lgs. 231/01).

- Associazione per delinquere (art. 416 c.p., ad eccezione del sesto comma);
- Associazione a delinquere finalizzata alla riduzione o al mantenimento in schiavitù, alla tratta di persone, all'acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 d.lgs. 286/1998 (art. 416, sesto comma, c.p.);
- Associazione di tipo mafioso (art. 416-bis c.p.);
- Scambio elettorale politico-mafioso (art. 416-ter c.p.);
- Sequestro di persona a scopo di estorsione (art. 630 c.p.);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 9 ottobre 1990, n. 309);
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo

guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo[18] (art. 407, co. 2, lett. a), numero 5, c.p.p.).

Reati commessi nei rapporti con la Pubblica Amministrazione (art. 25, d.lgs. 231/01).

- Concussione (art. 317 c.p.);
- Corruzione per l'esercizio della funzione (art. 318 c.p.);
- Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.);
- Corruzione in atti giudiziari (art. 319-ter c.p.);
- Induzione indebita a dare o promettere utilità (art. 319 quater c.p.);
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);
- Istigazione alla corruzione (art. 322 c.p.).

Traffico di influenze illecite (art. 346 bis c.p.):**Reati di falso nummario (art. 25-bis, d.lgs. 231/01)** Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);

- Alterazione di monete (art. 454 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.);
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

Delitti contro l'industria e il commercio (art. 25-bis.1, D.lgs. 231/01).

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.);

[18] Escluse quelle denominate «da bersaglio da sala», o ad emissione di gas, nonché le armi ad aria compressa o gas compressi, sia lunghe sia corte i cui proiettili erogano un'energia cinetica superiore a 7,5 joule, e gli strumenti lanciarazzi, salvo che si tratti di armi destinate alla pesca ovvero di armi e strumenti per i quali la "Commissione consultiva centrale per il controllo delle armi" escluda, in relazione alle rispettive caratteristiche, l'attitudine a recare offesa alla persona.

- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.);
- Illecita concorrenza con minaccia o violenza" (art. 513-bis c.p.);
- Frodi contro le industrie nazionali (art. 514).

Reati societari (art. 25-ter, d.lgs. 231/01)

- False comunicazioni sociali (art. 2621 c.c.);
- Fatti di lieve entità (art. 2621 bis c.c.);
- False comunicazioni sociali in danno dei soci o dei creditor(art. 2622c.c.);
- Falso in prospetto (art. 2623, comma 1 e 2, c.c.) (l'art. 2623 è soppresso dal 12/01/2006 dalla Legge del 28/12/2005 n. 262 art. 34);Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624, comma 1 e 2, c.c.) (l'art. 2624 c.c. è stato abrogato dal decreto legislativo 27 gennaio 2010, art. 37, co. 34);
- Impedito controllo (art. 2625, comma 2, c.c.);
- Indebita restituzione di conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.)
- Formazione fittizia del capitale (art. 2632 c.c.);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- Corruzione tra privati (art. 2635 c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Aggiotaggio (art. 2637 c.c.);

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.).**Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (art. 25-quater, D.Lgs. 231/01**

Pratiche di mutilazione degli organi genitali femminili (art. 583-bis c.p.) (art. 25-quater. 1, D.Lgs. 231/01)

Delitti contro la personalità individuale (art. 25-quinquies, d.lgs. 231/01).

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
- Prostituzione minorile (art. 600-bis c.p.);
- Pornografia minorile (art. 600-ter c.p.);
- Detenzione di materiale pornografico (art. 600-quater);
- Pornografia virtuale (art. 600-quater.1 c.p.) [aggiunto dall'art. 10, L. 6 febbraio 2006 n. 38];
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.);

- Tratta di persone (art. 601 c.p.);
- Acquisto e alienazione di schiavi (art. 602 c.p.);
- Intermediazione illecita e sfruttamento del lavoro (art. 603 bis c.p.) .

Reati di abuso di mercato (art. 25-sexies, d.lgs. 231/01).

- Abuso di informazioni privilegiate (d.lgs. 24.02.1998, n. 58, art. 184);
- Manipolazione del mercato (d.lgs. 24.02.1998, n. 58, art. 185).

Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies, d.lgs. 231/01).

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose (art. 590 c.p.).

Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies, d.lgs. 231/01).

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648-ter c.p.).

Delitti in materia di violazione del diritto d'autore (art. 25-novies, d.lgs. 231/01).

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, l. 633/1941 comma 1 lett. a) bis);
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l’onore o la reputazione (art. 171, l. 633/1941 comma 3);
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis l. 633/1941 comma 1);

- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis l. 633/1941 comma 2);
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter l. 633/1941);
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies l. 633/1941);
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies l. 633/1941).

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies, d.lgs. 231/01.

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

Reati ambientali (art. 25-undecies, D.lgs. 231/01).

- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.);
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.);
- Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (D.Lgs 152/06, art. 137);
- Attività di gestione di rifiuti non autorizzata (D.Lgs 152/06, art. 256);

- Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D.Lgs 152/06, art. 257);
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D.Lgs 152/06, art. 258);
- Traffico illecito di rifiuti (D.Lgs 152/06, art. 259);
- Attività organizzate per il traffico illecito di rifiuti (D.Lgs 152/06, art. 260);
- False indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; Omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (D.Lgs 152/06, art. 260-bis);
- Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. 150/92, art. 1 e art. 2);
- Inquinamento doloso (D.Lgs. 202/07, art. 8);
- Inquinamento colposo (D.Lgs. 202/07, art. 9);
- Inquinamento ambientale (art. 452-bis C.P.);
- Disastro ambientale (art. 452-quater C.P.);
- Delitti colposi contro l'ambiente (art. 452 quinques C.P.);
- Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies C.P.);
- Delitti associativi aggravati (art. 452 octies C.P.).

Impiego di lavoratori irregolari (art. 25-duodecies).

- Promozione, direzione, organizzazione, finanziamento e trasporto di stranieri irregolari all'interno dello Stato Italiano (art. 12 D. Lgs. 286/1998);
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, D. Lgs. 286/1998).

Razzismo e xenofobia (art. 25-terdecies).

- Promozione di idee razziste, commissione o istigazione alla commissione di violenze o atti di discriminazione per motivi razziali, etnici, nazionali o religiosi (art. 3 L. 654/1975).

Tuttavia in seguito all'entrata in vigore del D.lgs. 21/2018 che -all'art. 7, comma 1 lett. c)- ha abrogato l'art. 3 L. 654/75 introducendo il nuovo reato di Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa nel Codice Penale all'art. 604 bis, senza, tuttavia, intervenire direttamente sul D.Lgs. 231/2001, si è creato un evidente difetto di coordinamento fra le due norme, con ciò potendo anche interpretarsi come una volontà tacita del legislatore di abrogare il reato presupposto.Per tale ragione, tale reato – peraltro residuale ed eventuale – non è stato trattato nel Modello dell'ente.

Frode in competizione sportiva, esercizio abusivo di attività di giuoco o di scommessa e giochi di azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies).

- Frote in competizione sportiva (art. 1 L. 401/1989):
- Esercizio abusivo dell'attività di giuoco o di scommessa (art. 4 L. 401/1989);
- Esercizio di giochi di azzardo a mezzo di apparecchi vietati (art. 110 L. 146/1931 TULPS).

Reati tributari (art. 25-quinquiesdecies).

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 e 3 d.lgs. 74/2000):
- false fatturazioni o creazione di documenti per operazioni inesistenti (art. 8 D. Lgs. 74/2000);
- occultamento o distruzione di scritture contabili (art. 10 D. Lgs. 74/2000);
- sottrazione fraudolenta al pagamento delle imposte (art. 11 D. Lgs. 74/2000).

I soggetti destinatari del Decreto

Sotto il profilo dei soggetti destinatari, la legge indica *"gli enti forniti di personalità giuridica, le società fornite di personalità giuridica e le società e le associazioni anche prive di personalità giuridica"* (art. 1, co. 2). Il quadro descrittivo è completato dall'indicazione, a carattere negativo, dei soggetti cui non si applica la legge, vale a dire *"lo Stato, gli enti pubblici territoriali nonché gli enti che svolgono funzioni di rilievo costituzionale"* (art. 1, co. 3). Come si vede, la platea dei destinatari è molto ampia e non sempre è identificabile con certezza la linea di confine, specialmente per gli Enti che operano nel settore pubblico. È indubbia, in proposito, la soggezione alla disciplina in argomento delle società di diritto privato che esercitino un pubblico servizio (in base a concessione, ecc.). Nei loro riguardi – come, del resto, nei confronti degli Enti pubblici economici – la problematica della responsabilità riguarda, tra le altre comuni a tutti i destinatari della legge, anche le ipotesi di corruzione sia attiva che passiva[19]. È opportuno ricordare che questa nuova responsabilità sorge soltanto in occasione della realizzazione di determinati tipi di reati da parte di soggetti legati a vario titolo all'ente e solo nelle ipotesi in cui la condotta illecita sia stata realizzata nell'*interesse* o *a vantaggio* di esso, quindi non soltanto quando il comportamento illecito abbia determinato un vantaggio, patrimoniale o meno, per l'Ente, ma anche nell'ipotesi in cui, pur in assenza di tale concreto risultato, il fatto-reato trovi ragione nell'interesse dell'Ente.

Le sanzioni previste

Le sanzioni previste a carico dell'Ente sono le seguenti:

[19] È utile a questo proposito segnalare una decisione della Corte di Cassazione, che ha affermato che la disciplina *de qua* si applica esclusivamente a soggetti collettivi ovvero soggetti a struttura organizzata e complessa, escludendo così espressamente le ditte individuali dall'ambito di applicazione (cfr. Cass. VI Pen. sent. n. 18941/2004).

- **sanzione pecuniaria:** è determinata sulla base della gravità del reato commesso e del grado di responsabilità riconosciuto al soggetto giuridico tenuto conto delle attività poste in essere dall'ente per mitigare o prevenire la commissione d'illeciti. Della sanzione pecuniaria, il cui ammontare massimo previsto è pari a circa 1.550.000,00 Euro, risponde soltanto l'Ente con il suo patrimonio o con il fondo comune;
- **sanzioni interdittive** quali:
    - interdizione dall'esercizio dell'attività solitamente per un periodo compreso fra i tre mesi e i due anni; in casi particolarmente gravi tale sanzione può essere adottata anche in via definitiva. L'interdizione può essere disposta dal giudice anche in via cautelare in caso vi fossero concreti elementi che possano far ritenere concreto il pericolo di commissione di illeciti analoghi a quello già compiuto
    - sospensione o revoca di autorizzazioni, licenze e concessioni relative alla commissione dell'illecito
    - divieto di contrarre con la P.A.
    - esclusione o revoca di finanziamenti, contributi e sussidi
    - divieto di pubblicizzare beni e servizi
    - confisca del prezzo o del profitto derivante dal reato commesso
    - pubblicazione della sentenza

Ancor prima che sia accertata la responsabilità dell'Ente, il Pubblico Ministero può, in via preventiva, chiedere al Giudice, in presenza di particolari condizioni, l'applicazione di misure cautelari che, in attesa che vengano accertati i fatti, possono produrre gli stessi effetti di una sentenza di condanna.
L'ambito di applicazione dell'impianto sanzionatorio previsto dal D.lgs. 231/2001 opera anche nel caso in cui il reato sia rimasto a livello di tentativo (art. 26).
L'impianto sanzionatorio previsto dal D.lgs. 231/2001 opera anche nel caso siano intervenute operazioni straordinarie, quali trasformazione, fusione, scissione, cessione o conferimento di azienda o ramo d'azienda, sulla base della regola dell'inerenza e permanenza dell'eventuale sanzione interdittiva con il ramo di attività nel cui contesto sia stato commesso il reato.
Per quanto concerne la sanzione pecuniaria, in caso siano intervenute operazioni straordinarie quali scissioni, cessioni e conferimenti di ramo d'azienda, gli Enti beneficiari della scissione (totale o parziale), il cessionario e il conferitario sono solidalmente obbligati al pagamento della sanzione nei limiti del valore effettivo del patrimonio netto scisso o dell'azienda trasferita/conferita, salvo il caso di scissione di ramo d'attività nell'ambito del quale è stato commesso il reato, che determina una responsabilità esclusiva in capo allo specifico ramo d'azienda scisso.
Per gli altri casi di operazioni straordinarie, quali trasformazioni e fusioni (propria e per incorporazione), la responsabilità patrimoniale permane in capo all'Ente risultante (o incorporante) dall'operazione straordinaria.

La condizione esimente

L'articolo 6 del Decreto prevede una forma di esonero della responsabilità dell'Ente dai reati previsti qualora l'Ente dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, un *modello di organizzazione, gestione e controllo* idoneo a prevenire i reati della specie di quello eventualmente verificatosi e abbia incaricato un apposito organismo indipendente di vigilare affinché questo modello fosse osservato e continuamente aggiornato.

In modo specifico, il Decreto ha quindi previsto una forma specifica di esonero da tale responsabilità:

- presenza di modelli organizzativi e gestionali che possano sovrintendere alla prevenzione dei reati previsti dal Decreto
- presenza di un organismo (c.d. Organismo di Vigilanza o OdV) dell'Ente specificatamente dotato della funzione di vigilare sul funzionamento e sull'applicazione del Modello
- non vi sia stata omessa o insufficiente vigilanza da parte dell'OdV
- il soggetto che ha commesso il reato abbia eluso fraudolentemente il sistema di vigilanza e gestione

È stabilito quindi nel Decreto che il suddetto Modello di organizzazione, gestione e controllo debba rispondere alle esigenze di:

- identificazione delle aree nel cui ambito può verificarsi uno dei reati previsti
- individuazione di protocolli specifici con i quali programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire
- identificazione delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati
- imposizione di informazione nei confronti dell'organismo indipendente deputato a vigilare sull'osservanza del modello
- introduzione di un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello

L'adozione e l'efficace attuazione del presente Modello consente dunque agli Enti di beneficiare dell'esimente prevista dal Decreto e di limitare il rischio di commissione dei reati.

Il Decreto prevede che il Modello di organizzazione, gestione e controllo, possa essere adottato sulla base di codici di comportamento redatti dalle associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni, osservazioni sull'idoneità del modello nella prevenzione dei reati (cfr. D.lgs. 231/01, art. 6 comma 3).

In particolare, per adempiere la previsione di cui all'art. 6 Confindustria ha costituito a giugno 2001 un gruppo di lavoro che, dopo un'analisi sia delle prassi diffuse seguite negli ordinamenti in cui è diffusa l'adozione di codici di comportamento sia di quelle adottate dalle realtà aziendali italiane più importanti, ha predisposto le Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231/01.

La Giunta di Confindustria ha approvato le *Linee Guida*, in data 7 marzo 2002 (integrate nell'ottobre 2002 con un'appendice sui reati societari, aggiornate al marzo 2014) volte a definire i punti fondamentali per l'individuazione delle aree a rischio di commissione reato e la predisposizione del sistema di controllo adeguato a prevenire la commissione di tali reati, seguendo la previsione di legge richiamata al paragrafo precedente (art. 6).

In definitiva si possono identificare due ambiti d'intervento:

- identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in forma quali/quantitativa la possibilità di verificarsi dei reati previsti
- progettazione di un sistema di controllo (nella legge identificati come "protocolli") ossia il sistema organizzativo dell'Ente in grado di prevenire e contrastare efficacemente i rischi identificati, in modo tale che possa essere aggirato solo in modo fraudolento

Il sistema di controllo definito da Confindustria prevede:

- l'adozione di un Codice Etico;
- un sistema organizzativo adeguato sotto il profilo della definizione dei compiti, delle deleghe e delle procure;
- un sistema di procedure manuali ed informatiche;
- un sistema di controllo di gestione che possa segnalare tempestivamente situazioni di criticità, con particolare attenzione alla gestione dei flussi finanziari;
- un sistema di poteri autorizzativi e di firma assegnati in coerenza con le responsabilità organizzative e gestionali definite, prevedendo, quando richiesto, una puntuale indicazione delle soglie di approvazione delle spese;
- una efficace comunicazione del modello al personale e la sua formazione.

Queste componenti del sistema di controllo devono prevedere principi di:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione
- applicazione del principio di separazione delle funzioni
- documentazione dei controlli
- previsione di un adeguato sistema sanzionatorio per la violazione delle norme del codice etico e delle procedure previste dal Modello
- autonomia, indipendenza, professionalità e continuità d'azione dell'organismo di vigilanza

Per rendere effettivo tale sistema di prevenzione è necessario istituire un sistema sanzionatorio disciplinare, applicabile ai lavoratori dipendenti e ai collaboratori esterni, in grado di svolgere una funzione deterrente contro le violazioni delle prescrizioni aziendali.

Una parte qualificante del modello riguarda, infine, l'istituzione dell'Organismo di Vigilanza, un organismo di controllo, che deve vigilare sull'effettivo funzionamento del modello e che, in caso di inadeguatezza, deve proporre alle funzioni interessate i cambiamenti necessari.

È opportuno comunque evidenziare che le Linee Guida non sono vincolanti e che i Modelli predisposti dagli Enti possono discostarsi (senza che ciò pregiudichi l'efficacia dei Modelli stessi) in virtù della necessità di adattamento alle singole realtà organizzative.

In sintesi, le Società che dimostrano di avere un modello organizzativo adeguato non sono ritenute responsabili dei reati commessi dalla singola persona fisica.

Adozione del modello organizzativo

Obiettivi del modello

La Philogen, al fine di garantire sempre condizioni di correttezza e trasparenza dal punto di vista etico e normativo, ha ritenuto opportuno dotarsi di un Modello Organizzativo con il quale conseguire i seguenti obiettivi:

- implementare un sistema strutturato e organico di procedure e attività da porre in essere per prevenire la commissione dei reati previsti dal Decreto;
- coinvolgere, attraverso l'adozione del Modello e del Codice Etico, tutti i Destinatari affinché nello svolgimento delle proprie mansioni rispettino i principi etici cui è ispirata la Philogen;
- definire l'Organismo di Vigilanza che svolgerà le funzioni di sorveglianza riguardo l'efficacia e l'adeguatezza del Modello;
- individuare e attribuire responsabilità e poteri ad ogni unità organizzativa tenendo presente il rispetto del principio della separazione delle funzioni, in base al quale nessun soggetto può svolgere in completa autonomia un intero processo gestionale o decisionale;
- predisporre le attività necessarie ad un periodico aggiornamento del Modello.

A monte dell'adozione del modello e delle sue successive revisioni, Philogen ha svolto un'attività di rilevazione delle aree di rischio (*risk assessment*) sulla base di quanto previsto dal Decreto e sulle indicazioni presenti nelle "Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.lgs. 231/2001" elaborate da Confindustria. Tale attività ha avuto l'obiettivo di effettuare una mappatura preliminare delle funzioni aziendali e delle relative attività esposte a rischio di reato (c.d. *As is Analysis*) e valutare quali azioni porre in essere per far fronte alle criticità emerse (c.d. *Gap Analysis*). Il *risk assessment* definito a monte della prima stesura del Modello nel dicembre 2010 è stato in questa fase ridefinito tenendo conto dei provvedimenti messi in atto a seguito della messa in opera del Modello e sulla base degli aggiornamenti normativi intervenuti.

Nell'ambito del progetto di predisposizione del Modello la Philogen si è dotata di un Codice Etico volto a definire una serie di principi di "deontologia aziendale" che le società riconoscono come propri e dei quali esige l'osservanza da parte degli organi societari, dei propri dipendenti e di tutti coloro che cooperano a qualunque titolo al perseguimento dei fini aziendali.

Il Codice Etico ha pertanto una portata di carattere generale e rappresenta uno strumento adottabile anche in via autonoma da parte di Philogen. Il Modello, invece, risponde a specifiche prescrizioni contenute nel D.lgs. 231/2001, finalizzate a prevenire la

commissione di particolari tipologie di reati (per fatti che, apparentemente commessi a vantaggio della Società, possono far sorgere a carico della stessa una responsabilità amministrativa da reato in base alle disposizioni del Decreto medesimo).

Tuttavia, in considerazione del fatto che il Codice Etico richiama principi di comportamento idonei anche a prevenire i comportamenti illeciti di cui al D.lgs. 231/2001, esso acquisisce rilevanza ai fini del Modello e costituisce, pertanto, elemento rilevante del Modello medesimo.

Struttura del documento

Il presente documento è costituito da due sezioni distinte:

- **Parte Generale** che accoglie al suo interno la definizione delle caratteristiche generali afferenti al Modello Organizzativo con particolare attenzione ai seguenti aspetti:
  - la definizione dell'Organismo di Vigilanza e delle sue funzioni;
  - la definizione del sistema organizzativo e di controllo interno;
  - la formazione del personale e la diffusione del modello organizzativo in azienda e presso tutti i soggetti portatori di interesse verso la Philogen;
  - la definizione del sistema disciplinare e della sua applicazione.

- **Parti speciali** relative alle diverse tipologie di reato previste dal Decreto. In particolare la **Parte Speciale "A"** fa riferimento ai reati verso la PA, la **Parte Speciale "B"** è dedicata ai reati societari, la **Parte Speciale "C"** si occupa dei reati ambientali mentre la **Parte Speciale "D"** si occupa dei reati connessi alla sicurezza del lavoro e la **Parte Speciale "E"** si occupa dei reati informatici e il trattamento illecito di dati.
- Sono parte integrante del Modello Organizzativo i seguenti documenti:
  - il Codice Etico;
  - il documento di risk assessment, con la mappatura delle aree a rischio;
  - le procedure interne definite e richiamate nelle parti speciali.

Approvazione del Modello e suo recepimento nell'ambito del Gruppo

Il presente Modello, costituito dalla Parte Generale e dalla Parte Speciale, è stato approvato dal Consiglio di Amministrazione di Philogen con delibera del 5 Ottobre 2021.

Detto Modello si applica alla Società Philogen e non viene recepito automaticamente da parte delle altre società del Gruppo.

È demandato ai Consigli di Amministrazione delle diverse Società del Gruppo di provvedere mediante apposita delibera al recepimento del presente Modello organizzativo nonché delle parti speciali, in funzione dei profili di rischio configurabili nelle attività svolte dalle Società stesse e in accordo alle normative vigenti nei paesi in cui esse operano.

Qualora i Consigli di Amministrazione delle singole Società del Gruppo decidessero di recepire il Modello organizzativo della Philogen, hanno la possibilità di:

- istituire un proprio Organismo di Vigilanza ex art. 6, co. 1, lett. b), con tutte le relative attribuzioni di competenze e responsabilità. E' fatta salva la possibilità di attribuire questa funzione direttamente al Cda dirigente della controllata (così come previsto dall'art. 6, co. 4, D.Lgs. n. 231/2001);
- l'Organismo di Vigilanza/CdA della controllata può avvalersi, nell'espletamento del compito di vigilare sul funzionamento e l'osservanza del Modello, delle risorse allocate presso l'analogo Organismo della Capogruppo, sulla base di un predefinito rapporto contrattuale con la stessa;
- l'Organismo di Vigilanza della Capogruppo, nella effettuazione di controlli presso le Società del Gruppo, assume nella sostanza la veste di professionista esterno che svolge la sua attività nell'interesse della controllata stessa, riportando all'Organismo di Vigilanza/CdA di quest'ultima, con i vincoli di riservatezza propri del consulente esterno.

Modifiche e integrazioni del Modello

Essendo il Modello un atto di emanazione del CdA (in conformità alle prescrizioni dell'art. 6, primo comma, lettera a) del decreto legislativo) le successive modifiche e integrazioni di carattere sostanziale del Modello stesso sono rimesse all'approvazione del Consiglio di Amministrazione di Philogen.

È peraltro riconosciuta all'Amministratore Delegato e/o ai Consiglieri Delegati la facoltà di apportare al testo eventuali modifiche o integrazioni di carattere formale.

Metodologia seguita per l'individuazione delle attività sensibili e dei processi di supporto

L'art. 6.2 lett. a) del D.lgs. 231/01 indica, come uno dei requisiti del Modello, l'individuazione delle cosiddette "aree sensibili" o "a rischio", cioè di quei processi e di quelle aree di attività aziendali in cui potrebbe determinarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.lgs. 231/01.

È stata analizzata la realtà operativa aziendale nelle aree/settori aziendali in cui è possibile la commissione dei reati previsti dal D.lgs. 231/01, evidenziando i momenti ed i processi maggiormente rilevanti.

Parallelamente, è stata condotta un'indagine sugli elementi costitutivi dei reati in questione, allo scopo di identificare le condotte concrete che, nel contesto aziendale, potrebbero realizzare le fattispecie delittuose.

L'iter metodologico seguito dalla Philogen per la realizzazione del Modello di organizzazione, gestione e controllo ex Decreto Legislativo 231/2001 è scomponibile nelle seguenti fasi:

- **Fase di Scoping**: definizione dettagliata del perimetro oggetto di valutazione e individuazione, attraverso questionari specifici rivolti ai soggetti apicali, dei corretti processi aziendali e dei relativi referenti;
- **Fase di Analisi**: valutazione del sistema di controllo interno in essere, raccolta, mediante interviste ed analisi documentale, delle informazioni necessarie a costruire la mappa delle principali attività a rischio reato e l'elenco delle possibili modalità di realizzazione dei comportamenti configurati come reati e per i quali sia prevista una responsabilità della Società ai sensi del Decreto Legislativo, analisi e valutazione dei punti di debolezza individuati, determinazione dei possibili rimedi.

Individuazione delle attività a rischio reato

Al fine di individuare specificatamente e in concreto le aree di attività a rischio di commissione di reato (di seguito "attività "a rischio" o "sensibili") si è proceduto a un'analisi della struttura societaria e organizzativa di Philogen.

Le risultanze della fase di analisi sono state riportate nel *risk assessment* definito nella sua prima stesura nel dicembre 2010 e successivamente rivisto. In sintesi, con riferimento alle fattispecie di reati suscettibili di configurare la responsabilità amministrativa della società, sono state identificate le aree di attività "a rischio" (dettagliatamente analizzate nella Parte Speciale) che sono state distinte tra quelle che fanno riferimento a:

- Rapporti con la Pubblica Amministrazione;
- Reati societari;
- Reati ambientali;
- Sicurezza e prevenzione degli infortuni sul lavoro e tutela dell'igiene e della salute sul lavoro.

Rapporti con la Pubblica Amministrazione

Le aree di attività potenzialmente "a rischio" riferite ai rapporti con la Pubblica Amministrazione sono qui di seguito elencate:

- Gestione dei contratti con ospedali, medici e opinion leader coinvolti nelle sperimentazioni cliniche;
- Gestione dei rapporti con funzionari pubblici per adempimenti normativi ed in occasione di verifiche e ispezioni sul rispetto della normativa medesima;

- Gestione dei rapporti con le Autorità nell'ambito dello svolgimento delle sperimentazioni cliniche ed in relazione al processo produttivo;
- Richiesta, gestione, monitoraggio di finanziamenti agevolati, contributi, esenzioni fiscali, formazione finanziata, ecc.

Reati societari

Le attività amministrative e contabili di Philogen che risultano potenzialmente "sensibili" e che fanno riferimento in larga parte ai reati societari sono oggetto di analisi periodiche dettagliate da parte del controllo di gestione interno, della Società di revisione e del Collegio Sindacale.

Nello specifico, con riferimento ai postulati di bilancio (esistenza e accadimento, completezza, valutazione e misurazione, diritti e obblighi, presentazione e informativa) e all'adeguatezza della segregazione dei compiti e ruoli, sono stati analizzati i seguenti processi aziendali (e i relativi sotto processi):

- Ciclo attivo
- Ciclo passivo
- Ciclo di magazzino
- Ciclo degli investimenti
- Cedolini e gestione del personale
- Tesoreria, cassa, banche e movimentazioni finanziarie
- Imposte e tasse
- Chiusura contabile
- Consolidamento

Reati ambientali

Le aree di attività "a rischio" o "sensibili" con riferimento al potenziale reato ambientale si riferiscono all'area produttiva della Società e in particolare allo smaltimento dei rifiuti tossici derivanti dagli scarti biologici dell'area produttiva. Trattandosi di alcuni dei reati previsti di natura colposa investono i vari tipi di società in maniera "oggettiva" e quindi rilevano anche per l'attività di Philogen.

Sicurezza e prevenzione degli infortuni sul lavoro e tutela dell'igiene e della salute sul lavoro

L'introduzione della Legge 3 agosto 2007, n. 123 (art. 25-septies), nell'impianto normativo del D.lgs. n. 231/2001 ha portato a un'analisi accurata relativa alla gestione degli adempimenti prescritti dalla Legge n. 626/1994 ripreso nel cosiddetto Testo Unico Sicurezza Lavoro (d.lgs. 81/2008), a sua volta successivamente integrato dal D.lgs. n. 106

del 3 agosto 2009 in materia di sicurezza e prevenzione degli infortuni sul lavoro e tutela dell'igiene e della salute sul lavoro. Trattandosi di reati di natura colposa anch'essi investono ogni tipo di società in maniera "oggettiva" e quindi rilevano anche per l'attività di Philogen.

Applicazione del Modello da parte delle singole società

È attribuita alla responsabilità delle singole Società del Gruppo l'attuazione del Modello nel proprio ambito, riguardo alle attività dalle stesse in concreto poste in essere nelle aree a rischio.

L'Organismo di Vigilanza (OdV)

Descrizione

Il Decreto e la relativa relazione di accompagnamento dispongono che l'Organismo di Vigilanza debba rispondere alle seguenti caratteristiche:

- **Autonomia ed indipendenza**: l'OdV non deve essere direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto del suo controllo. Inoltre deve essere garantita all'OdV la più elevata indipendenza gerarchica e la possibilità di riportare al Consiglio di Amministrazione;
- **Professionalità**: l'OdV deve presentare al suo interno figure la cui professionalità e competenza sono rispondenti al ruolo che devono svolgere;
- **Continuità d'azione**: l'OdV deve operare costantemente con la vigilanza e con l'aggiornamento, ove necessario, del Modello.

Sono nel seguito riassunti gli elementi fondamentali relativi all'attività dell'Organismo di Vigilanza, maggiormente dettagliati nel documento "*Regolamento dell'Organismo di Vigilanza*".

Composizione e nomina

I componenti dell'OdV sono scelti fra soggetti qualificati ed esperti in ambito legale, contabile e societario, dotati di professionalità e competenza e degli opportuni requisiti di onorabilità tali da garantire imparzialità nel giudizio e autorevolezza ed eticità di condotta.

Le seguenti motivazioni costituiscono causa d'ineleggibilità a membro dell'OdV:

- interdizione, inabilitazione, fallimento o condanna a una pena che comporti l'interdizione anche temporanea dai pubblici uffici ovvero l'incapacità di esercitare uffici direttivi;
- condanna per aver commesso uno dei reati previsti dal Decreto.

L'OdV nomina, in accordo con il Consiglio di Amministrazione, il Referente Interno che svolge funzioni operative di raccordo fra Philogen e l'Organismo, questi ha il compito operativo di accompagnare l'OdV sia nei controlli che nelle verifiche sul rispetto e l'adeguatezza del Modello.

Il Consiglio di Amministrazione ha confermato quale Organismo di Vigilanza Monocratico il Dott. Marco Tanini in data 26/04/2016.

È stato altresì indicato quale Referente Interno . L'Avv. Patrizia Sacchi.

Funzioni e poteri

Le funzioni dell'Organismo di Vigilanza previste dal Decreto e dalle linee guida fornite da Confindustria si riassumono come segue:

- verificare l'osservanza di quanto contenuto nel Modello Organizzativo da parte dei destinatari (come specificati nel seguito del Modello Organizzativo);
- controllare l'adeguatezza e l'efficacia del Modello in merito alla capacità di prevenzione dei reati previsti dal Decreto;
- appurare la necessità/opportunità di apportare modifiche e aggiornamenti al Modello.

Si tratta di attività che richiedono non solo le competenze tecniche necessarie al loro corretto svolgimento ma presuppongono che siano svolte con continuità di azione.

L'OdV definisce e svolge le attività di sua competenza ed è dotato di "autonomi poteri d'iniziativa e controllo" secondo quanto indicato dal decreto all'art. 6. In particolare:

- l'OdV gode di completa autonomia nell'azione di verifica dell'efficacia e dell'effettiva attuazione del Modello, considerando comunque che il CdA della Società è incaricato di valutare l'adeguatezza del suo intervento;
- l'OdV ha libero accesso presso tutte le funzioni della Società senza la necessità di fornire preavviso alcuno al fine di ottenere informazioni o dati necessari allo svolgimento dei suoi compiti.
- gode, oltre ad un compenso stabilito dal CdA, di una dotazione finanziaria (budget) dettagliata nei documenti programmatici dell'OdV e quindi nel piano operativo da presentare all'organo amministrativo.

I flussi informativi da e verso l'organismo di vigilanza

L'OdV deve essere tempestivamente informato da tutti i Destinatari del Modello di qualsiasi notizia concernente l'esistenza di possibili violazioni dello stesso.

A tal proposito sono istituiti opportuni canali informativi con l'obiettivo di facilitare il flusso di segnalazioni/informazioni verso l'OdV. :tali canali saranno definiti dall'OdV stesso.

In ogni caso, devono essere obbligatoriamente e immediatamente trasmesse all'OdV le informazioni:

A) che possono avere attinenza con violazioni, anche potenziali, del Modello, incluse, senza che ciò costituisca limitazione:
   - le notizie relative alla commissione dei reati in specie all'interno di Philogen o dei soggetti terzi che possono impegnare la Società nei confronti della Pubblica Amministrazione a pratiche non in linea con le norme di comportamento indicate nel Modello;

- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura proceda per i reati previsti dalla richiamata normativa;
- eventuali ordini ricevuti dal superiore e ritenuti in contrasto con la legge, la normativa interna, o il Modello;
- eventuali richieste od offerte di doni (eccedenti il valore modico) o di altre utilità provenienti da pubblici ufficiali o incaricati di pubblico servizio;
- eventuali omissioni, trascuratezze o falsificazioni nella tenuta della contabilità o nella conservazione della documentazione su cui si fondano le registrazioni contabili;
- i provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità dai quali si evinca lo svolgimento di indagini che interessano, anche indirettamente, il Gruppo, i suoi dipendenti o i componenti degli organi sociali;
- le richieste di assistenza legale inoltrate alla società dai dipendenti ai sensi del CCNL, in caso dell'avvio di un procedimento penale a carico degli stessi;
- le notizie relative ai procedimenti disciplinari in corso e alle eventuali sanzioni irrogate ovvero la motivazione della loro archiviazione.

B) che, relativamente all'attività della Philogen, possono assumere rilevanza per l'OdV nell'espletamento dei compiti ad esso assegnati, incluse, senza che ciò costituisca limitazione:
   - i rapporti predisposti dai responsabili delle funzioni dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D.Lgs. 231/2001;
   - le notizie salienti relative ai cambiamenti organizzativi;
   - gli aggiornamenti del sistema dei poteri e delle deleghe;
   - le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
   - i prospetti riepilogativi delle gare, pubbliche o a rilevanza pubblica, a livello nazionale/locale cui la Philogen ha partecipato e ottenuto la commessa; nonché i prospetti riepilogativi delle commesse eventualmente ottenute a seguito di trattativa privata.

L'OdV, nel corso dell'attività d'indagine che segue alla segnalazione, deve agire in modo da garantire che i soggetti coinvolti non siano oggetto di ritorsioni, discriminazioni o, comunque, penalizzazioni, assicurando, quindi, la riservatezza del soggetto che effettua la segnalazione (salvo la ricorrenza di eventuali obblighi di legge che impongano diversamente).

Philogen, al fine di facilitare le segnalazioni all'OdV da parte dei soggetti che vengano a conoscenza di violazioni del Modello, anche potenziali, attiva gli opportuni canali di comunicazione dedicati e, precisamente:

- un’apposita casella di posta elettronica interna accessibile dalla rete aziendale (odv@philogen.it);
- tramite posta interna in busta chiusa da inviare all’attenzione dell’Organismo di Vigilanza presso la Segreteria di Philogen Spa;
- attraverso l’utilizzo di della cassetta della posta posizionata nel refettorio della sede amministrativa Philogen di Rosia.

L’OdV effettua inoltre un’attività di reporting agli organi societari con cui:

- riferisce oralmente, su base almeno semestrale all’Amministratore Delegato ed al Collegio Sindacale sull’attività compiuta e sull’esito della stessa;
- relaziona per iscritto, su base annuale, al Consiglio di Amministrazione, all’Amministratore Delegato ed al Collegio Sindacale sull’attività compiuta nel periodo e sull’esito della stessa, fornendo un piano di attività previste per l’anno successivo.

L’attività di reporting avrà a oggetto, in particolare:

- l’attività svolta dall’OdV;
- le eventuali criticità (con spunti di miglioramento) emerse sia in termini di comportamenti o eventi interni alla Società, sia in termini di efficacia del Modello;
- i correttivi, necessari o eventuali, da apportare al fine di assicurare l’efficacia e l’effettività del Modello;
- l’accertamento di comportamenti non in linea con il Modello;
- la rilevazione di carenze organizzative o procedurali tali da esporre la Società al pericolo che siano commessi reati rilevanti ai fini del Decreto;
- l’eventuale mancata o carente collaborazione da parte delle funzioni aziendali nell’espletamento dei propri compiti di verifica e/o d’indagine;
- in ogni caso, qualsiasi informazione ritenuta utile ai fini dell’assunzione di determinazioni urgenti da parte degli organi deputati;
- rendiconto delle spese sostenute;
- eventuali mutamenti del quadro normativo che richiedono un aggiornamento del Modello.

Gli incontri devono essere verbalizzati e le copie dei verbali devono essere conservate presso gli uffici dell’OdV.

L’attività di controllo dell’OdV si svolge altresì attraverso eventuali rapporti straordinari richiesti dagli Organi societari in dipendenza di eventi di particolare rilievo.

Rapporti con altri organi e funzioni aziendali

L'OdV, si coordinerà con le altre funzioni aziendali per lo svolgimento di compiti che richiedono specifiche competenze e conoscenze del funzionamento dell'azienda.

In particolare, si coordinerà con:

- gli organi/funzioni aziendali coinvolti nell'implementazione degli interventi eventualmente necessari per l'adeguamento alle disposizioni del d.lgs. 231/2001;
- la funzione legale per l'interpretazione della normativa rilevante e la raccolta delle segnalazioni che perverranno dalle strutture della società e da soggetti terzi.

Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, report previsti nel presente Modello sono conservati dall'OdV per un periodo di dieci anni.

L'accesso all'archivio è consentito ai componenti dell'OdV, all'Amministratore Delegato e del Collegio Sindacale.

Il sistema organizzativo e di controllo interno

Il sistema organizzativo e di controllo interno di un'azienda è strettamente legato ai suoi processi, al modo con cui vengono governati e alla loro integrazione.

Nella progettazione e implementazione di un adeguato sistema di controllo occorre tenere in considerazione una serie di fattori tra loro strettamente legati, quali:

- struttura organizzativa ed ambiente;
- valutazione dei rischi;
- controlli e loro efficacia/efficienza;
- sistema delle comunicazioni;
- sistema di monitoraggio.

Ambiente di controllo

In questo contesto intenderemo per “ambiente di controllo” l’insieme degli individui costituenti l’azienda, con le proprie qualità, i propri valori etici e le proprie competenze, e dell’ambiente nel quale essi operano.

I fattori che influenzano l’ambiente di controllo sono:

- integrità, valori etici e competenza del personale;
- filosofia e stile gestionale del management;
- modalità di delega delle responsabilità;
- capacità di indirizzo e guida del Consiglio di Amministrazione;
- organizzazione e sviluppo professionale del personale;
- organi di controllo interni ed esterni.

Organizzazione della società

Assemblea degli azionisti. È competente a deliberare in sede ordinaria e straordinaria sulle materie alla stessa riservate dalla legge o dallo Statuto sociale.

Consiglio di Amministrazione. È investito dei più ampi poteri per l’amministrazione della Società, con facoltà di compiere tutti gli atti opportuni per il raggiungimento degli scopi sociali, ad esclusione degli atti riservati – dalla legge o dallo Statuto – all’Assemblea.

Collegio Sindacale. Ha il compito di vigilare:

- sull’osservanza della legge e dello Statuto nonché sul rispetto dei principi di corretta amministrazione;
- sull’adeguatezza della struttura organizzativa della Società, del sistema di controllo interno e del sistema amministrativo contabile, anche in riferimento all’affidabilità di quest’ultimo nel rappresentare correttamente i fatti di gestione;
- sulle modalità di concreta attuazione delle regole di governo societario previste da codici di comportamento redatti da società di gestione di mercati regolamentati o da associazioni di categoria, cui la società, mediante informativa al pubblico dichiara di attenersi;
- sull’adeguatezza delle disposizioni impartite alle società controllate in relazione alle informazioni da fornire per adempiere agli obblighi di comunicazione;
- sul processo di informativa contabile, sulla revisione legale dei conti e sull’indipendenza della società di revisione legale.

Società di Revisione Legale

L’attività di revisione legale dei conti viene svolta da una Società specializzata appositamente nominata dall’Assemblea degli Azionisti previo parere espresso dal

Collegio Sindacale. È stata all'uopo confermata con atto del 26 aprile 2016 la Società KPMG S.p.A.

Struttura di *governance* di Philogen

Il sistema di governo societario adottato dalla Società si pone quale obiettivo primario la creazione di valore per gli azionisti, nella consapevolezza della rilevanza della trasparenza sulle scelte e sulla formazione delle decisioni aziendali, nonché della necessità di predisporre un efficace sistema di controllo interno.

Si riportano di seguito i principali strumenti di *governance* di cui la Società si è dotata anche in osservanza delle più recenti disposizioni normative e regolamentari, delle previsioni del Codice e della *best practice* nazionale e internazionale:

- Statuto;
- Codice etico;
- Regolamento dell'Organismo di Vigilanza;
- Procedure interne.

Il codice etico

Philogen ha definito il proprio Codice Etico per evidenziare i valori etici fondamentali ai quali s'ispira e ai quali tutti i dipendenti e collaboratori esterni (consulenti, agenti, prestatori di servizi) si devono attenere nello svolgimento dei compiti e funzioni loro affidate.

I principi contenuti nel Codice Etico si applicano a tutti i dipendenti e ai collaboratori esterni.

La molteplicità d'interessi e contesti socio-economici con cui l'Azienda interagisce, unitamente alle modalità di organizzazione, impongono l'impegno di tutti per assicurare che le attività dell'Azienda siano svolte nell'osservanza della legge, in un quadro di concorrenza leale, con onestà, integrità, correttezza e buona fede, nel rispetto degli interessi legittimi dei clienti, dipendenti, partner commerciali e finanziari e delle collettività in cui l'Azienda è presente con le proprie attività.

È stato pertanto opportuno ribadire, con la stesura del Codice Etico, a tutti coloro che lavorano nell'Azienda o che operano per il conseguimento dei suoi obiettivi l'importanza di osservare e di fare osservare questi principi nell'ambito delle proprie funzioni e responsabilità.

In nessun modo la convinzione di agire per il bene di Philogen può giustificare l'adozione di comportamenti in contrasto con questi principi.

L’osservanza delle norme del Codice Etico deve considerarsi parte essenziale delle obbligazioni contrattuali dei dipendenti e collaboratori esterni dell’Azienda ai sensi e per gli effetti di legge.

Come tale il Codice Etico è consegnato puntualmente a tutti i dipendenti, fornitori e collaboratori.

Philogen garantisce specifiche procedure per la segnalazioni di fatti illeciti (violazioni di legge, reati o altre irregolarità) da parte dei propri dipendenti e collaboratori, di cui siano venuti a conoscenza nell’ambito dello svolgimento delle proprie funzioni lavorative, salvaguardandone l’anonimato, prevedendo appositi canali per la segnalazioni circonstanziate di violazioni del modello di organizzazione e gestione dell'ente; tali canali, anche informatici, garantiscono la riservatezza dell’identità del segnalante nelle attivita' di gestione della segnalazione.

Il Regolamento dell’Organismo di Vigilanza

L’organismo di vigilanza (OdV), al fine di svolgere in maniera più efficace ed efficiente le proprie attività, può adottare un Regolamento interno che stabilisce le procedure operative da seguire per eseguire al meglio la propria funzione.

Il Regolamento, redatto dai suoi membri ed approvato a maggioranza all’interno dell’Organismo, per la sua validità è soggetto alla preventiva approvazione da parte del C.d.a.

Le procedure interne

Le procedure aziendali sono formalizzate all’interno del Sistema di Gestione della Qualità (SGQ) di cui la società è dotata,

Esse sono approvate, emanate e revisionate periodicamente secondo pecise modalità, dettagliate nel Manuale di Gestione.

In particolare Philogen, in attuazione di quanto previsto dall’art. 2 della L. 179/2017 che ha allargato la disciplina del “Whistleblowing” anche al settore privato, inserendolo nell’art. 6 del D. Lgs. 231/2001, si impegna ad implementare specifiche procedure per la segnalazioni di violazioni di legge, reati o altre irregolarità da parte dei propri dipendenti e collaboratori, di cui siano venuti a conoscenza nell’ambito dello svolgimento delle proprie funzioni lavorative, salvaguardandone l’anonimato, prevedendo appositi canali per la segnalazioni circonstanziate di violazioni del modello di organizzazione e gestione dell'ente.

Tali canali, anche ma non solo informatici, garantiscono la riservatezza dell'identità del segnalante nelle attivita' di gestione della segnalazione.

La Philogen, in attuazione dei principi previsti dalla direttiva UE 2019/1937, pubblicata nella Gazzetta della Unione Europea il 26.11.2019 e non ancora recepita nell'ordinamento italiano - il quale ha due anni di tempo per farlo – intende ampliare le figure tutelate dalla disciplina, comprendendo oltre a manager e dipendenti, anche i soggetti esterni (quali lavoratori autonomi, tirocinanti, personale sotto la direzione di appaltatori e fornitori).

Consiglio di Amministrazione
Nomina

La Società è amministrata da un Consiglio di Amministrazione composto di un numero di membri non inferiore a due e non superiore a nove. L'Assemblea, di volta in volta, prima di procedere all'elezione del Consiglio, ne determina il numero dei componenti entro i limiti suddetti.

Gli Amministratori, che possono non essere soci, durano in carica per un periodo non superiore a tre esercizi e sono rieleggibili a norma dell'art. 2383 del Codice Civile.

La nomina degli amministratori è effettuata dall'Assemblea ordinaria.

Attuale Composizione

Il Consiglio di Amministrazione, è stato rinnovato con atto del 26 aprile 2016 e composto di sei amministratori che rimarranno in carica fino all'approvazione del bilancio di esercizio al 31 dicembre 2018.

Nome e cognome	**Carica**
Duccio Neri	Presidente e Amministratore Delegato
Dario Neri	Consigliere
Giovanni Neri	Consigliere Delegato
Sergio Gianfranco Luigi Maria Dompe'	Consigliere
Nathalie Francesca Maria Dompe'	Consigliere
Roberto Marsella	Consigliere
Leopoldo Zambeletti	Consigliere
Guido Guidi	Consigliere
Roberto Ferraresi	Consigliere

Ruolo e compiti

La gestione della Società spetta esclusivamente al Consiglio di Amministrazione, il quale compie le operazioni necessarie per l'attuazione dell'oggetto sociale.

Oltre ad esercitare i poteri che gli sono attribuiti dalla legge, il Consiglio di Amministrazione è competente a deliberare in merito alle seguenti materie:

- adeguamento dello Statuto alle disposizioni normative;
- operazioni di fusione per incorporazione o di scissione della Società ai sensi degli artt. 2505, 2505 bis e 2506 ter, ultimo comma, del codice civile;
- l'istituzione o la soppressione di sedi secondarie;
- la riduzione del capitale sociale in caso di recesso di uno o più soci;
- il trasferimento della sede sociale nel territorio nazionale.

Il Consiglio può attribuire, modificare e revocare deleghe, definendone con chiarezza e precisione i limiti e le modalità di esercizio.

Amministratori esecutivi

Il Consiglio di Amministrazione può delegare proprie attribuzioni a un comitato esecutivo, nominando un Amministratore delegato. Il Consiglio può altresì nominare uno o più Vice Presidenti.

La carica di Amministratore Delegato è stata conferita al consigliere Duccio Neri, il quale può stipulare contratti di ogni tipo e genere, ivi compresi quelli richiedenti la forma scritta a pena di nullità nonché assumere e licenziare operai, impiegati, quadri e dirigenti; assumere finanziamenti bancari per conto della Società, sotto qualsiasi forma e per qualsiasi importo, accettare e utilizzare i crediti concessi da detti Istituti, rilasciare agli Istituti stessi effetti cambiari senza limite d'importo e accettare le condizioni e i patti tutti inerenti a quant'altro da essi richiesto; contrarre mutui e in genere impegnare la Società in operazioni finanziarie con o senza garanzia, reale o personale; comprare e trasferire beni immobili, il tutto con esonero dei competenti Conservatori dei Registri Immobiliari e delle Ipoteche; rappresentare la Società nei confronti delle pubbliche Amministrazioni e, a titolo esemplificativo, dell'Intendenza di Finanza, Poste, Dogane, Ferrovie, Tesorerie Provinciali e Comunali, Uffici delle Imposte, Ministeri, Direzioni e uffici da essi dipendenti; promuovere azioni giudiziarie e resistere in giudizio nominando procuratori *ad lites* e avvocati. All'Amministratore Delegato è inoltre conferito il potere di nominare mandatari con minori o uguali poteri nonché procuratori ad negozia per determinati atti o categorie di atti. Il Dott. Duccio Neri è munito di tutti i poteri per l'ordinaria e straordinaria amministrazione e per il buon andamento degli affari sociali.

Ai sensi dello Statuto sociale, gli organi delegati curano che l'assetto organizzativo, amministrativo e contabile sia adeguato e riferiscono al Consiglio di Amministrazione e al Collegio Sindacale almeno ogni sei mesi su tali argomenti, sul generale andamento della gestione e sulla sua prevedibile evoluzione, nonché sulle operazioni di maggior rilievo effettuate dalla Società e dalle sue controllate.

Amministratori non esecutivi

Il Consiglio si compone in parte di componenti non esecutivi (in quanto sprovvisti di deleghe operative e/o di funzioni direttive in ambito aziendale) tali da garantire per numero e autorevolezza che il loro giudizio possa avere un peso significativo nell'assunzione di decisioni consiliari.

Gli Amministratori non esecutivi apportano le loro specifiche competenze nelle discussioni consiliari, in modo da favorire un esame degli argomenti in discussione secondo prospettive diverse e una conseguente adozione di deliberazioni meditate, consapevoli e allineate con l'interesse sociale.

Sistema di controllo interno

Elementi essenziali del sistema di controllo interno

Il Consiglio di Amministrazione, con l'assistenza dell'Organismo di Vigilanza definisce le linee d'indirizzo del sistema di controllo interno, in modo che i principali rischi afferenti alla Società e alle sue controllate siano correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati, determinando inoltre criteri di compatibilità di tali rischi con una sana e corretta gestione dell'impresa.

Il sistema di controllo interno è l'insieme delle regole, delle procedure e delle strutture, organizzative volte a consentire, attraverso un adeguato processo d'identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati.

Gli elementi essenziali del sistema di controllo interno possono essere descritti con riferimento alle seguenti componenti:

In materia di controllo interno la Società ha un apposito sistema, cui è affidata la missione

- di accertare l'adeguatezza dei diversi processi aziendali in termini di efficacia, efficienza ed economicità, nonché
- di garantire l'affidabilità e la correttezza delle scritture contabili e la salvaguardia del patrimonio aziendale e

- di assicurare la conformità degli adempimenti operativi alle normative interne ed esterne e alle direttive ed indirizzi aziendali aventi la finalità di garantire una sana ed efficiente gestione.

Il sistema di controllo interno si articola nell'ambito della Società in due distinte modalità:

- il "controllo di linea", costituito dall'insieme delle attività di controllo che le singole unità operative svolgono sui propri processi. Tali attività di controllo sono demandate alla responsabilità primaria del management operativo e sono considerate parte integrante di ogni processo aziendale;
- l'auditing esterno, demandato alla società KPMG per le attività di revisione legale dei conti ai sensi dell'articolo 13 del D.Lgs 39/2010;
- Il collegio sindacale secondo quanto previsto dall'articolo 2403 del Codice Civile.

Il Consiglio di Amministrazione ha confermato il dott. Duccio Neri quale Amministratore esecutivo incaricato di sovrintendere alla funzionalità del sistema di controllo interno.

Sono compiti dell'Amministratore esecutivo incaricato di sovrintendere alla funzionalità del sistema di controllo interno:

- curare l'identificazione dei principali rischi aziendali, tenendo conto delle caratteristiche delle attività svolte dalla Società e dalle sue controllate, e sottoporli periodicamente all'esame del Consiglio di Amministrazione;
- dare esecuzione alle linee di indirizzo definite dal Consiglio di Amministrazione, provvedendo alla progettazione, realizzazione e gestione del sistema di controllo interno, verificandone costantemente l'adeguatezza complessiva, l'efficacia e l'efficienza e adattando tale sistema alla dinamica delle condizioni operative e del panorama legislativo e regolamentare.

Inoltre, con l'introduzione del nuovo Codice della Crisi (D. Lgs. 14/2019), è stato modificato l'art. 2086 del c.c. che ora prevede l'obbligo, per l'imprenditore che operi in forma societaria, di adottare un adeguato assetto organizzativo, amministrativo e contabile, con l'obiettivo di rilevare tempestivamente una eventuale crisi dell'impresa ed attivare di conseguenza uno o più degli strumenti previsti dal nostro ordinamento per superare la crisi (concordato preventivo, accordo di ristrutturazione dei debiti….).
In questo contesto, il il sistema di controllo interno dovrà prevedere:

- Idonee procedure che permettano di rilevare tempestivamente le informazioni amministrativo- contabili necessarie per intercettare i segnali di crisi;
- Adozione di strumenti informatici che consentano la raccolta e la gestione delle informazioni di cui al punto precedente, fedelmente e tempestivamente in modo da poter informare l'organo di controllo sull'esistenza dei cosiddetti "indizi della crisi".

Gli strumenti adottati a tali fini dovranno fornire i dati necessari per elaborare i cosiddetti indici significativi della possibile crisi di impresa, che dovranno misurare e monitorare:

- la sostenibilità degli oneri dell'indebitamento con i flussi di cassa che l'impresa è in grado di generare;
- l'adeguatezza dei mezzi propri rispetto a quelli di terzi;
- il livello dei ritardi nei pagamenti dei fornitori.

Società di Revisione

L'attività di revisione contabile è effettuata da KPMG S.p.A. nominata dall'Assemblea ordinaria degli Azionisti in data 26/04/2016 preso atto della proposta espressa dal Collegio Sindacale.

L'Organismo di Vigilanza

L'Organismo di Vigilanza è istituito ai sensi dell'art. 6, comma 1, lett. b), del Decreto, con il precipuo scopo di vigilare sul rispetto delle disposizioni contenute nel Modello, allo scopo di prevenire i reati che possano originare un profilo di responsabilità amministrativa/penale in capo alla Società.

Il citato art. 6 del Decreto prevede che l'ente possa essere esonerato dalla responsabilità conseguente alla commissione dei reati indicati se il CdA ha, fra l'altro: adottato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati; affidato il compito di vigilare sul funzionamento e l'osservanza del Modello Organizzativo e di curarne l'aggiornamento a un organismo dell'ente dotato di autonomi poteri d'iniziativa e controllo (l'Organismo di Vigilanza). L'affidamento di detti compiti all'Organismo e, ovviamente, lo svolgimento degli stessi sono, dunque, presupposti indispensabili per l'esonero dalla responsabilità.

Si rimanda al capitolo "Organismo di Vigilanza" del presente documento per i dettagli riguardanti l'istituzione e al funzionamento del predetto Organismo.

Collegio sindacale

Nomina

Il Collegio Sindacale è composto di tre membri effettivi e due supplenti.

I Sindaci effettivi e i Sindaci supplenti sono nominati dall'Assemblea sulla base di liste presentate dagli azionisti, nelle quali i candidati devono essere elencati mediante un numero progressivo e devono risultare in numero non superiore ai componenti dell'organo da eleggere.

Per i poteri e doveri dei Sindaci si osservano le norme di legge, regolamentari e di vigilanza di tempo in tempo vigenti.

Attuale composizione

Il Collegio Sindacale in carica, rinnovato con atto del 07 maggio 2019 fino alla data dell'approvazione del bilancio al 31 dicembre 2020, è così composto:

Membri	Carica
Stefano Mecacci	Presidente
Pierluigi Matteoni	Sindaco Effettivo
Marco Tanini	Sindaco Effettivo
Ernico De Bernardi	Sindaco Supplente
Antonella Candelieri	Sindaco Supplente

Ruolo e compiti

Oltre ai compiti attribuitegli dalla legge, il Collegio Sindacale, tramite incontri periodici, provvede alla supervisione sull'operato della Società di Revisione e inoltre approva preventivamente l'affidamento alla Società di Revisione di ulteriori incarichi da parte della Società o di società del Gruppo, nel rispetto delle disposizioni del d.lgs. 27 gennaio 2010 n. 39.

Nel corso della propria attività il Collegio, tra l'altro vigila sull'indipendenza della Società di Revisione, verificando tanto il rispetto delle disposizioni normative in materia, quanto la natura e l'entità dei servizi diversi dal controllo contabile prestati alla Società e alle sue controllate da parte della stessa società di revisione e delle entità appartenenti alla rete medesima.

Assemblea

Nella convocazione, nella programmazione e nella gestione delle adunanze assembleari, particolare attenzione viene rivolta a favorire la massima partecipazione da parte degli Azionisti, nonché a garantire il massimo livello qualitativo dell'informativa agli stessi offerta in tali circostanze, nel rispetto dei vincoli e delle modalità di diffusione inerenti alle informazioni price sensitive.

La convocazione dell'Assemblea, sia ordinaria che straordinaria, è fatta con pubblicazione, secondo le modalità e nei termini previsti dalla normativa applicabile, dell'avviso contenente le indicazioni del giorno, dell'ora e del luogo dell'adunanza, l'elenco degli argomenti da trattare nonché le ulteriori informazioni previste dalla legge e dalle disposizioni regolamentari applicabili. Ai sensi dell'art. 16 dello Statuto Sociale, coloro che hanno diritto di intervenire all'Assemblea possono farsi rappresentare con delega scritta da altro soggetto nei limiti e nelle modalità previste dall'articolo 2372 del Codice Civile.

Formazione del personale e diffusione del documento

Ai fini dell'attuazione del presente Modello, è obiettivo di Philogen garantire una corretta conoscenza, sia alle risorse già presenti in azienda sia a quelle da inserire, delle regole di condotta ivi contenute, con differente grado di approfondimento sul diverso livello di coinvolgimento delle risorse medesime nei processi sensibili.

Il sistema d'informazione e formazione è supervisionato e integrato dall'attività realizzata in questo campo dall'Organismo di Vigilanza in collaborazione con il responsabile della Funzione Risorse Umane e con i responsabili delle altre funzioni di volta in volta coinvolte nell'applicazione del Modello.

La comunicazione iniziale

L'adozione del presente Modello è comunicata a tutte le risorse presenti in azienda al momento dell'adozione stessa. Tutte le modifiche intervenute in seguito e le informazioni concernenti il Modello verranno comunicate a tutti i destinatari utilizzando adeguati canali informativi. Ai nuovi assunti, invece, viene consegnato un set informativo (es. Codice Etico, Modello organizzativo, Regolamento informatico, Autorizzazione del trattamento dei dati ai fini della Privacy ex D. Lgs. 196/2003) per assicurare agli stessi le conoscenze considerate di primaria rilevanza.

La formazione

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D. Lgs. 231/2001 è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della Società. In particolare, Philogen prevede livelli diversi d'informazione e formazione attraverso strumenti di divulgazione quali, a titolo esemplificativo, periodici seminari mirati, occasionali e-mail di aggiornamento, note informative interne.

Informativa verso collaboratori esterni e partners

Saranno fornite a soggetti esterni alla Società (consulenti, partner e fornitori) apposite informative sulle politiche e le procedure adottate da Philogen sulla base del presente Modello, nonché i testi delle clausole contrattuali abitualmente utilizzate al riguardo.

I soggetti esterni devono essere informati del contenuto del Modello e dell'esigenza della Società che il loro comportamento sia conforme ai disposti del D.lgs. 231/2001.

Nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.) che operano con la Pubblica Amministrazione o coinvolte nello svolgimento di attività a rischio rispetto ai reati societari per conto o nell'interesse della Philogen, i relativi contratti devono:

- essere definiti per iscritto, in tutte le loro condizioni e termini;
- contenere clausole standard, condivise con la Funzione Legale della Società, al fine del rispetto del d.lgs. 231/2001;
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al d.lgs. 231/2001 e di impegnarsi a tenere comportamenti conformi al dettato della norma;
- contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al d.lgs. 231/2001 (es. clausole risolutive espresse, penali).

Sistema disciplinare

Principi generali

Il D.lgs. 231/2001 stabilisce esplicitamente all'art. 6 che l'azienda deve porre in essere un adeguato sistema disciplinare al fine di sanzionare comportamenti non rispondenti alle misure indicate dal Modello.

Costituisce violazione del Modello Organizzativo la messa in atto di comportamenti che rispondano ai seguenti requisiti:

- omissione o violazione delle direttive presenti nel Modello nell'espletamento delle proprie attività;
- esposizione dell'azienda a rischio di commissione di reati previsti dal Decreto;
- non rispondenza ai principi contenuti nel Codice Etico della Società.

In particolare l'istituzione di un sistema sanzionatorio commisurato alle possibili violazioni risponde a un duplice scopo:

- aumentare le probabilità di efficacia del Modello stesso, fungendo da deterrente per le violazioni;
- rafforzare l'efficacia dell'azione di controllo operata dall'OdV.

L'applicazione delle sanzioni è indipendente rispetto all'avvio o all'esito di un eventuale procedimento avviato presso le Autorità Giudiziarie competenti.

A tal fine Philogen prevede una graduazione delle sanzioni applicabili, sul differente grado di pericolosità che i comportamenti possono presentare rispetto alla commissione dei reati. È stato stilato pertanto un sistema disciplinare che sanzioni tutte le infrazioni al Modello, dalla più grave alla più lieve, mediante un sistema di gradualità della sanzione che, secondariamente, rispetti il principio della proporzionalità tra la mancanza rilevata e la sanzione comminata.

Per garantire l'efficacia del sistema sanzionatorio è necessario che ogni violazione del Modello e delle procedure stabilite in attuazione dello stesso da chiunque commesse devono essere immediatamente comunicate all'OdV.

Ai sensi dell'art. 7 dello Statuto dei Lavoratori[20] il disciplinare che prevede il sistema di sanzioni di seguito descritto, per essere valido ed efficacie, deve essere affisso all'interno della Società affinché sia portato a conoscenza di tutti i Destinatari. Il sistema disciplinare è parte integrante del seguente documento ed è di seguito riportato.

In applicazione di quanto previsto dall'art. 6 del D. Lgs. 231/2001 nella parte che ha introdotto l'obbligo per l'impresa di adottare un sistema di segnalazione di condotte illecite o di violazioni del modello di organizzazione e gestione dell'ente, sono state introdotte

[20] Legge 20 maggio 1970, n. 300 Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento.

specifiche sanzioni disciplinari per chi dovesse violare la riservatezza dei segnalanti e/o per chi dovesse porre in essere atti di ritorsione o discriminatori, diretti od indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione. Sono parimenti previste specifiche sanzioni disciplinari per chi dovesse effetttuare, con dolo o colpa grave, segnalazioni infondate.

L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni può in ogni caso essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale maggiormente rappresentativa all'interno dell'ente.

Condotte rilevanti

Ai fini del Sistema Disciplinare aziendale, nel rispetto delle previsioni contenute nel CCNL, laddove applicabili, costituiscono condotte oggetto di sanzione le azioni o i comportamenti posti in essere in violazione del Modello. Essendo quest'ultimo costituito anche dal complesso delle procedure che ne sono parte integrante, ne deriva che per "violazione del Modello" deve intendersi anche la violazione di uno o più procedure.

In considerazione dell'obbligo gravante, a mente del Codice Etico di Philogen, su ciascun destinatario di ottemperare alle indicazioni e/o alle prescrizioni provenienti dall'Organismo di Vigilanza (OdV), costituiscono violazioni del Modello anche le condotte, ivi incluse quelle omissive, poste in essere in violazione delle indicazioni e/o delle prescrizioni dell'OdV.

Nel rispetto del principio costituzionale di legalità, nonché di quello di proporzionalità della sanzione, tenuto conto di tutti gli elementi e/o delle circostanze ad essa inerenti, si ritiene opportuno definire un elenco di possibili violazioni, graduate secondo un ordine crescente di gravità:

1) mancato rispetto del Modello, qualora si tratti di violazioni in cui non ricorra una delle condizioni previste nei successivi punti 2 e 3;

2) mancato rispetto del Modello, qualora si tratti di una violazione idonea ad integrare il solo fatto (elemento oggettivo) di uno dei reati previsti nel Decreto;

3) mancato rispetto del Modello, qualora si tratti di violazione finalizzata alla commissione di uno dei reati previsti dal Decreto, o comunque sussista il pericolo che sia contestata la responsabilità della Società ai sensi del Decreto;

4) mancato rispetto del principio di riservatezza e tutela del segnalante in caso di segnalazioni di eventi illeciti o violazioni del MOGC fatti da dipendenti ai sensi della L. 179/2017, c.d. whistleblowing;

5) esecuzione di atti ritorsivi e/o discriminatori nei confronti di chi abbia effettuato (in buona fede) una segnalazione inerente condotte illecite, rilevanti ai sensi del Decreto 231 e/o

violazioni del modello, di cui i destinatari siano venuti a conoscenza in ragione delle funzioni svolte.

6) trasmissione di segnalazioni di violazioni di legge o del MOGC ai sensi della L. 179/2017 che si siano rivelate poi infondate, qualora siano state effettuate con dolo o colpa grave.

Sanzioni per operai, impiegati e quadri

Il sistema disciplinare è applicato nei confronti dei lavoratori dipendenti con qualifica di operaio, impiegato e quadro con riferimento a quanto previsto dall'art. 7 della Legge 20 maggio 1970 n. 300 (Statuto dei lavoratori) e ai vigenti CCNL per i lavoratori dipendenti.

Il Modello costituisce un complesso di norme cui il personale dipendente di Philogen deve uniformarsi anche ai sensi di quanto previsto dai rispettivi CCNL in materia di norme comportamentali e di sanzioni disciplinari.

La violazione delle previsioni del Modello e delle procedure di attuazione comporta l'applicazione del procedimento disciplinare e delle relative sanzioni, ai sensi di Legge e dei citati CCNL.

In particolare, in applicazione delle "Norme comportamentali e disciplinari" richiamati dal CCNL, si prevedono le seguenti sanzioni disciplinari:

Ammonizioni scritte, multe e sospensioni nel caso di:

- violazione delle procedure interne previste dal presente Modello;
- omissione di controllo o tolleranza di lievi comportamenti irregolari;
- omissione di comunicazione all'OdV delle informazioni prescritte;
- adozione di comportamenti non conformi alle prescrizioni del modello stesso, dovendosi ravvisare in tali comportamenti una "esecuzione con negligenza del lavoro affidatogli[21]".

Licenziamento per mancanze nel caso di:

- adozione nell'espletamento delle attività nelle aree a rischio di un comportamento giudicato gravemente non conforme alle prescrizioni del Modello;
- compimento di atti contrari all'interesse della Philogen o che arrechino danno o espongano i beni aziendali ad una situazione di oggettivo pericolo, dovendosi ravvisare in tali comportamenti una "trascuratezza nell'adempimento degli obblighi contrattuali o di regolamento interno";
- adozione nell'espletamento delle attività nelle aree a rischio di un comportamento palesemente in violazione delle prescrizioni del presente Modello, tale da determinare la concreta applicazione a carico della società di misure previste dal Decreto, dovendosi ravvisare in tali comportamenti una condotta tale da provocare

[21] Art.51 del CCNL

all'azienda "grave nocumento morale e/o materiale", nonché da costituire "azioni delittuose" a termine di Legge così come richiamato nel CCNL.

L'applicazione del tipo e dell'entità delle sanzioni sopra richiamate è dipendente dai seguenti fattori:

- INTENZIONALITÀ di porre in essere il comportamento;
- RECIDIVA, ovvero dall'eventuale presenza di precedenti disciplinari posti in essere in passato contro il dipendente;
- GRADO DI RESPONSABILITÀ del lavoratore.

Il sistema disciplinare è costantemente monitorato dall'OdV e dal Responsabile delle Risorse Umane.

Sanzioni per i Dirigenti

Nei casi in cui la violazione riguardi un Dirigente, l'Organismo di Vigilanza deve darne comunicazione all'Amministratore Delegato e al Consiglio di Amministrazione mediante relazione scritta.

I destinatari della comunicazione provvederanno ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal Contratto Collettivo Nazionale del Lavoro applicabile.

In particolare sono previste le seguenti sanzioni:

- ammonizioni scritte, multe e sospensioni nel caso di lieve commissione delle seguenti azioni;
- violazione delle procedure interne previste dal presente Modello (ad es. non osservi le procedure prescritte per le aree esposte a rischio di commissione di reato);
- omissione di controllo o tolleranza di comportamenti irregolari tenuti dal personale
- omissione di comunicazione all'OdV delle informazioni prescritte;
- adozione di un comportamento non conforme alle prescrizioni del Modello stesso.

Licenziamento ex art. 2118 c.c. nel caso di

- comportamento giudicato gravemente non conforme alle prescrizioni del Modello nell'espletamento delle attività nelle aree a rischio;
- atti contrari all'interesse della Philogen o che arrechino danno o espongano i beni aziendali ad una situazione di oggettivo pericolo;
- comportamento non conforme alle prescrizioni del Modello tale da configurare una possibile esecuzione di un reato previsto dal Decreto con particolare riferimento alle attività svolte nelle aree a rischio.

Licenziamento per giusta causa nel caso di

- comportamento palesemente in violazione delle prescrizioni del Modello nell'espletamento delle attività nelle aree a rischio, tale da comportare la concreta applicazione a carico della società di misure previste dal Decreto riconducibile ad una condotta tale da provocare all'azienda "grave danno morale e/o materiale".

Sanzioni per gli Amministratori

Nei casi in cui la violazione riguardi un Amministratore delle Società, l'Organismo di Vigilanza deve darne immediata comunicazione al Consiglio di Amministrazione e al Collegio Sindacale, mediante relazione scritta.

Nei confronti degli Amministratori che abbiano commesso una violazione del Modello o delle procedure stabilite in attuazione dello stesso, il Consiglio di Amministrazione può applicare ogni idoneo provvedimento consentito dalla Legge, tra i quali le seguenti sanzioni, determinate a seconda della gravità del fatto e della colpa e delle conseguenze che ne sono derivate per la società:

- richiamo formale scritto;
- sanzione pecuniaria pari all'importo da due a cinque volte gli emolumenti calcolati su base mensile;
- revoca, totale o parziale, delle eventuali procure;
- convocazione dell'Assemblea con proposta di revoca della carica.

Sanzioni per Collaboratori esterni

Nei casi in cui si verifichino fatti che possono integrare violazione del Modello da parte di collaboratori o controparti contrattuali, l'Organismo di Vigilanza informa l'Organo Amministrativo, il Responsabile del Personale e il Responsabile di Funzione alla quale il contratto o il rapporto si riferisce, mediante relazione scritta.

I contratti stipulati con questi soggetti devono contenere specifiche clausole risolutive espresse che possano essere applicate dalla società nel caso di comportamenti in contrasto con le linee di condotta indicate nel Modello e tali da comportare il rischio di commissione di un reato sanzionato dal Decreto.

Rapporti infragruppo

Ogni prestazione di servizi svolta da altre società del gruppo a favore o nell'interesse della Philogen viene regolata da un apposito contratto di servizio. Tale contratto disciplina le condizioni, i criteri e i modi dell'erogazione del servizio di volta in volta considerato, nonché i criteri di fatturazione del medesimo e le garanzie di qualità ed eticità che la sua erogazione nell'interesse di Philogen deve soddisfare.

Tali contratti disciplinano, fra l'altro:

- la garanzia di conformità del servizio al d.lgs. 231/2001, al Codice Etico aziendale e alle procedure correlate, sanzionando i comportamenti contrari alle suddette previsioni;
- le modalità operative specifiche di ciascun servizio;
- i criteri e le modalità contabili per determinare gli importi che l'azienda beneficiaria del servizio è tenuta a corrispondere all'azienda erogatrice;
- la qualità del servizio erogato.

PARTE SPECIALE “A”

Reati in danno della Pubblica Amministrazione

relativa al

Modello di Organizzazione, Gestione e Controllo

Reati contro la Pubblica Amministrazione

Definizione di Pubblica Amministrazione

I reati contro la Pubblica Amministrazione sono disciplinati dal Titolo II, del Libro secondo, del Codice Penale.

Il Decreto individua, fra le diverse fattispecie, le ipotesi corruttive, nelle varie forme, di malversazione ai danni dello Stato e d'indebita percezione di erogazioni pubbliche, cui si aggiungono la truffa ai danni dello Stato e la frode informatica, di cui agli artt. art. 640, II comma, n. 1, 640 bis e 640 ter c.p.

Il soggetto a cui nocumento è consumato il reato è quindi **la Pubblica Amministrazione, definita quale aggregazione** (secondo quanto stabilito dalla Relazione Ministeriale al Codice Penale) **di tutti gli Enti che "svolgono tutte le attività dello Stato e degli altri Enti pubblici" inclusi, quindi, anche gli Stati esteri, gli Organi Comunitari e le emanazioni estere dello Stato.**

Per PA s'intende, in estrema sintesi, l'insieme di Enti e Soggetti pubblici (Stato, Ministeri, Regioni, Province, Comuni, etc.) e talora privati (ad es., concessionari, amministrazioni aggiudicatrici ecc.) e tutte le altre figure che svolgono in qualche modo la funzione pubblica, nell'interesse della collettività e quindi nell'interesse pubblico. Oggetto della tutela penale nei reati che rilevano in questa sede è il regolare funzionamento nonché il prestigio degli Enti Pubblici e, in generale, quel'buon andamento' dell'Amministrazione di cui all'art. 97 della Costituzione, ovvero, nel caso dei reati di truffa, il patrimonio pubblico.

La nozione di Pubblico Ufficiale è fornita direttamente dal legislatore, all'art. 357 del c. p., il quale indica il "*pubblico ufficiale"* in "*chiunque eserciti una pubblica funzione legislativa, giudiziaria o amministrativa"*.

Diversamente, l'art. 358 c.p. riconosce la qualifica di ''*incaricato di un pubblico servizio*'' a tutti "*coloro i quali, a qualunque titolo, prestano un pubblico servizio''*.

Riportiamo nel seguito una breve descrizione dei reati contemplati negli artt. 24 e 25 del Decreto.

Truffa ai danni dello Stato e di altro ente pubblico (art. 640, comma 2, n.1, c.p.)

Essa si verifica quando, per ottenere ingiusti profitti, si mettono in atto raggiri o artifici tali da recare un danno allo Stato, ad altri Enti pubblici o all'UE.

Ad esempio: la società, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, fornisce alla P.A. informazioni non veritiere (ad esempio supportate da documentazione mendace), al fine di ottenere l'aggiudicazione della gara stessa.

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

È un'ipotesi specifica della Truffa in danno dello Stato o dell'UE e si concretizza quando la truffa è diretta a ottenere contributi, finanziamenti, mutui agevolati o altre erogazioni pubbliche.

Ad esempio: produzione di documenti falsi attestanti l'esistenza di requisiti inesistenti, necessari per ottenere il finanziamento pubblico.

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

Tale ipotesi di reato si configura nel caso in cui, dopo aver ricevuto finanziamenti o contributi da parte dello Stato italiano o altri Enti Pubblici o dall'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate. La condotta, infatti, consiste nel distrarre, anche parzialmente, la somma ottenuta, facendo rilevare che l'attività programmata si sia comunque svolta.

Il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che non siano destinati alle finalità per cui erano stati erogati.

Ad esempio: la società destina parte dei finanziamenti ricevuti per la formazione ad altro tipo di spese (es. per coprire spese di rappresentanza).

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

Tale ipotesi di reato si configura nei casi in cui, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione d'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 dall'Unione Europea. In questo caso, a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti. Tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato (vedi punto 6.1.1), nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

Ad esempio: la Società produce documenti falsi attestanti l'esistenza di requisiti inesistenti, necessari per ottenere il finanziamento pubblico. In particolare, potrebbe essere falsamente redatto un atto attestante l'esistenza di una garanzia fideiussoria. Tale documento, infatti, potrebbe essere indispensabile al fine di ottenere le erogazioni dal Fondo Sociale Europeo riguardo all'organizzazione di corsi di formazione per i dipendenti.

Frode informatica a danno dello Stato o di altro ente pubblico (art. 640 ter, comma 1 c.p.)

È una tipologia di reato oggi poco frequente ma è prevedibile che in futuro avrà sempre più ampia diffusione.

Si verifica quando viene alterato il funzionamento di un sistema informatico o i dati in esso contenuti al fine di procurare a sé o ad altri un profitto.

Ad esempio: alterazione di registri informatici della Pubblica Amministrazione al fine di far risultare condizioni necessarie per la partecipazione della Società a una gara pubblica.

Ostacolo alle funzioni ispettive e di vigilanza della Presidenza del Consiglio dei ministri in tema di sicurezza nazionale cibernetica (art. 11 L. 133/2019)

È una tipologia di reato nuova dovuta alla necessità di tutelare, per finalità di sicurezza nazionale, il c.d. "perimetro di sicurezza nazionale cibernetica", ovvero l'integrità e la sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale" (art. 1, comma 1, L. 133/2019).

Si verifica quando vengono fornite informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici impiegati (art. 1 co. 2 lett. b), o ai fini delle comunicazioni preventive al Centro di valutazione e certificazione nazionale (art. 1 co. 6 lett. a), o per lo svolgimento di specifiche attività ispettive e di vigilanza (co. 6 lett. c) ovvero omettere di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

Ad esempio: su richiesta dalla P.A. competente, si forniscono informazioni, dati o elementi di fatto non rispondenti al vero, da utilizzare per la predisposizione dell'elenco delle reti, dei sistemi informativi e dei servizi informativi necessari per il funzionamento di una funzione essenziale dello Stato.

Concussione (art. 317 c.p.)

È la condotta di un pubblico ufficiale o un incaricato di pubblico servizio che, abusando del suo potere, costringe qualcuno a dare o promettere a lui o a terzi denaro o altra utilità.

Ad esempio: la Società partecipa a una gara al fine di prestare i propri servizi a un Ente pubblico. È possibile che il funzionario pubblico ponga in essere comportamenti concussivi

in danno di terzi partecipanti al fine di avvantaggiare la Società medesima che, in questa ipotesi, concorre con i dipendenti dell'Ente pubblico nella condotta delittuosa.

La Concussione è caratterizzata dalla volontà prevaricatrice del P.U. cui consegua il condizionamento della volontà del privato.

Corruzione (artt. 318-319 c.p.)

Si verifica quando un pubblico ufficiale riceve denaro o altra utilità o la promessa degli stessi, per l'esercizio della propria funzione (corruzione impropria).

L'attività del pubblico ufficiale dovrà intendersi in senso lato e quindi in una vasta gamma di comportamenti, effettivamente o potenzialmente riconducibili all'incarico del pubblico ufficiale e quindi un vero e proprio asservimento di detto soggetto pubblico ai desiderata del soggetto privato, vista la non necessità di dimostrare un legame tra il compenso e uno specifico atto di ufficio.

Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco quindi i due soggetti si trovano in posizione di sostanziale parità, mentre nella concussione il privato subisce la condotta del pubblico ufficiale versando in uno stato di soggezione e dovendo sottostare alle ingiuste pretese del primo.

Ad esempio: al fine di aggiudicarsi una gara pubblica o di velocizzare la pratica, la società dà o promette denaro ai rappresentanti della Pubblica Amministrazione.

Lo stesso è punito il pubblico ufficiale che ritarda o omette un atto del suo ufficio o compie un atto contrario ai doveri del proprio ufficio.

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

La pena prevista per tale reato si applica a chiunque offra o prometta a un pubblico ufficiale o a un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, denaro o altra utilità, qualora la promessa o l'offerta non siano accettate.

Corruzione in atti giudiziari (art. 319-ter c.p.)

Il reato si configura nel caso in cui un soggetto offra o prometta a un pubblico ufficiale o a un incaricato di un pubblico servizio denaro o altra utilità al fine di favorire o danneggiare una parte in un processo civile, penale o amministrativo.

Potrà dunque essere chiamata a rispondere del reato la società che, essendo parte in un procedimento giudiziario, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere o altro funzionario) al fine di ottenerne la positiva definizione.

A completamento dell'esame dei reati previsti dall'art. 24 del Decreto, si evidenzia che, a norma dell'art. 322 bis. c.p., i suddetti reati sussistono anche nell'ipotesi in cui essi riguardino pubblici ufficiali stranieri, ossia coloro che svolgano funzioni analoghe a quelle dei pubblici ufficiali italiani nell'ambito di Organismi comunitari, di altri Stati membri dell'Unione Europea, di Stati esteri o organizzazioni pubbliche internazionali.

Induzione indebita a dare o promettere utilità (art. 319 quater)

Detto articolo prevede l'ipotesi residuale introdotta dalla Novella al codice penale nel 2012 dell'induzione indebita , ove il fatto non costituisca più grave reato. Si tratta quindi di una norma di chiusura a completamento del quadro normativo.

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

Sempre in tema di corruzione impropria l'art. 320 c.p., recentemente novellato, prevede l'ipotesi residuale della corruzione dell'incaricato di pubblico servizio.

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

La condotta consiste nello sfruttare, o vantarsi di sfruttare, relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio, per farsi indebitamente dare o promettere di dare, a sé o ad altri, denaro o altra utilità, quale prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio oppure per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri.

Aree a rischio

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione.

Sono quindi definite a rischio tutte le aree aziendali che per lo svolgimento della propria attività intrattengono rapporti con la Pubblica Amministrazione o gestiscono risorse finanziarie che potrebbero essere impiegate per attribuire vantaggi e utilità a pubblici ufficiali (c.d. "rischio indiretto").

In particolare, in seguito all'attività di *risk assessment* posta in essere in azienda sono state individuate le seguenti attività aziendali considerate a rischio diretto:

- Gestione dei contratti con ospedali, medici ed opinion leader coinvolti nelle sperimentazioni cliniche;
- Gestione dei rapporti con funzionari pubblici per adempimenti normativi ed in occasione di verifiche e ispezioni sul rispetto della normativa medesima;

- Gestione dei rapporti con le Autorità nell'ambito dello svolgimento delle sperimentazioni cliniche ed in relazione al processo produttivo;
- Richiesta, gestione, monitoraggio di finanziamenti agevolati, contributi, esenzioni fiscali, formazione finanziata, ecc.

Più in generale nella gestione dei rapporti con funzionari pubblici per adempimenti normativi e in occasione di verifiche e ispezioni sul rispetto della normativa medesima il cui ambito di rischio è:

- la gestione amministrativa (es: adempimenti fiscali, rapporti con uffici tributari, rapporti con CCIAA, ufficio del Registro, Guardia di Finanza, ecc.) e relative verifiche ispettive;
- la gestione del personale (es: rapporti con gli Enti previdenziali ed assistenziali, INPS, INAIL), la gestione delle convenzioni con Enti pubblici e relative verifiche ispettive;
- la gestione dei rapporti con funzionari pubblici (A.S.L., VVFF, Ispettorato del Lavoro, medico competente, etc.) per gli adempimenti prescritti dal Testo Unico Sicurezza Lavoro (d.lgs. 81/2008), anche in occasione di ispezioni/ verifiche.

Le aree che sono coinvolte dal **rischio indiretto** sono principalmente quelle inerenti:

- l'Amministrazione, Finanza e Controllo a fronte delle quali è necessario impedire l'accantonamento di somme di danaro a scopi corruttivi o fondi occulti;
- la gestione dei contratti di consulenza a fronte della quale è necessario impedire il rischio che gli incarichi dissimulino illecite attribuzioni di utilità.

Destinatari della parte speciale

La presente parte speciale si riferisce a comportamenti posti in essere da Amministratori, Dirigenti e dipendenti (nel seguito "Esponenti Aziendali") operanti nelle aree in cui vengono svolte attività a rischio nonché da Collaboratori esterni (di seguito tutti definiti i "Destinatari").

Principi generali di comportamento e di attuazione del processo decisionale nelle aree di attività a rischio

La presente parte speciale prevede l'espresso divieto, a carico degli Esponenti Aziendali, in via diretta, e a carico dei Collaboratori esterni, tramite apposite clausole contrattuali, di:

- porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto);
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Nell'ambito dei suddetti comportamenti è fatto divieto in particolare di:

- offrire o promettere di offrire a pubblici funzionari o loro parenti, amici o affini, denaro, doni o omaggi, salvo non si tratti di doni di utilità d'uso e modico valore così come previsto dalla vigente normativa e dai relativi codici di condotta;
- esaminare o proporre opportunità di impiego per i dipendenti della Pubblica amministrazione o a loro parenti, amici o affini;
- fornire o ottenere informazioni e/o documenti riservati da cui Philogen possa conseguire un indebito o illecito interesse e/o vantaggio;
- indurre Pubblici Ufficiali e/o Incaricati di pubblico servizio, italiani o esteri, ad utilizzare la loro influenza su altri soggetti appartenenti alla Pubblica Amministrazione italiana o estera;
- qualsiasi altro comportamento volto ad ottenere un vantaggio tale da compromettere l'integrità di una o entrambe le parti;
- riconoscere compensi in favore di Collaboratori Esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alla prassi vigente;
- presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- destinare somme ricevute da organismi pubblici nazionali comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
- porre comunque in essere comportamenti in violazione del Codice Etico da intendersi qui integralmente richiamato.

Ai fini dell'attuazione dei comportamenti di cui sopra:

- gli incarichi conferiti ai Collaboratori Esterni devono essere redatti per iscritto, con l'indicazione del compenso pattuito ed essere sottoscritti conformemente alle deleghe ricevute;
- nessun tipo di pagamento di importo rilevante può essere effettuato in contanti o in natura;
- le operazioni che comportano utilizzazione o impiego di risorse economiche o finanziarie hanno una causale espressa e sono documentate e registrate in conformità ai principi di correttezza contabile;
- la gestione dei rapporti con membri della P.A. deve essere gestita, quando sia possibile, con un adeguato turnover;
- le comunicazioni con la P.A. devono avvenire preferibilmente per iscritto;
- qualora la comunicazione avvenga attraverso supporti informatici, l'identità e l'idoneità dell'operatore che immette dati e dichiarazioni deve essere sempre individuabile;
- le dichiarazioni rese ad Organismi pubblici nazionali o comunitari ai fini dell'ottenimento di erogazioni, contributi o finanziamenti, devono contenere solo elementi assolutamente veritieri e, in caso di ottenimento degli stessi, deve essere rilasciato apposito rendiconto;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità;
- devono essere immediatamente segnalati all'Autorità Giudiziaria ed all'OdV eventuali comportamenti della controparte pubblica volte ad ottenere favori, elargizioni illecite di denaro o altre utilità nei confronti di terzi;
- devono essere segnalati tempestivamente all'OdV situazioni di conflitto di interesse anche potenziali, in particolare il soggetto che si trovi in tale situazione si astiene dal partecipare a decisioni in relazione alle quali possa determinarsi il predetto conflitto.

Aree di attività a rischio: elementi fondamentali del processo decisionale

Protocollo relativo all'attività con la Pubblica Amministrazione

Il seguente protocollo descrive le modalità operative da seguire nel caso in cui la Società si trovi a dover interagire con i rappresentanti della Pubblica Amministrazione (funzionari e amministratori) e deve essere seguito ogni qual volta Philogen vi entri in contatto.

I seguenti protocolli si riferiscono a ciascun Responsabile di funzione (nel seguito anche il "Responsabile") la cui area di attività determina un contatto diretto o indiretto con la Pubblica Amministrazione

A tal fine vanno osservate le seguenti disposizioni operative:

1. Il Responsabile deve garantire
    a) la tracciabilità dei rapporti e della gestione delle commesse con la Pubblica Amministrazione;
    b) il rispetto delle norme vigenti e delle regole di comportamento aziendali;
    c) il perseguimento dell'interesse aziendale.
2. Ogni attività a rischio deve essere portata a conoscenza dell'OdV dai suddetti responsabili.

Sulle operazioni in questione l'OdV potrà predisporre ulteriori controlli dei quali verrà data evidenza scritta.

Istruzioni e verifiche dell'OdV

In quest' ambito è inoltre compito dell'OdV:

1) verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe in vigore, raccomandando modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al responsabile interno o ai sub responsabili;
2) verificare periodicamente, con il supporto delle altre funzioni competenti, l'osservanza da parte dei Collaboratori esterni delle disposizioni del Decreto;
3) verificare periodicamente, con il supporto delle altre funzioni competenti, l'adeguatezza e la congruità degli incarichi ai Collaboratori Esterni;
4) verificare periodicamente, con il supporto anche della Società di revisione e delle altre funzioni competenti le richiesta, la gestione, il monitoraggio dei finanziamenti agevolati e contributi pubblici;
5) dare attuazione, con il supporto delle altre funzioni competenti, ai meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni;
6) indicare al Management le eventuali integrazioni ai sistemi di gestione finanziaria già presenti in Società, con l'evidenza degli accorgimenti opportuni a rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiore discrezionalità rispetto a quanto ordinariamente previsto.

Indicazioni finali

A completamento di quanto indicato nel presente paragrafo e per le indicazioni operative è possibile far riferimento alle seguenti procedure:

- **“Procedura di affidamento incarichi ai Collaboratori Esterni”;**
- **“Regolamento dell’OdV”.**

PARTE SPECIALE “B”

Reati societari

relativa al

Modello di Organizzazione, Gestione e Controllo

Reati societari

Si riporta di seguito una breve descrizione dei principali reati contemplati nell'art. 25-ter del Decreto la cui commissione possa comunque comportare un beneficio alla Società.

False comunicazioni sociali (artt. 2621 e 2622 c.c.)

Si tratta di due ipotesi criminose la cui condotta tipica coincide quasi totalmente e che si differenziano per il verificarsi o meno di un danno patrimoniale ai destinatari delle comunicazioni.

Le due fattispecie criminose si realizzano tramite l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla Legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, idonei a indurre in errore i destinatari della situazione economica, patrimoniale o finanziaria della Società o del Gruppo al quale essa appartiene, con l'intenzione di ingannare i soci, i creditori o il pubblico; ovvero l'omissione, con la stessa intenzione, d'informazioni sulla situazione medesima la cui comunicazione è imposta dalla Legge.

Si precisa che:

- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- le informazioni false o omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della Società e del Gruppo al quale essa appartiene;
- la responsabilità si estende anche all'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla Società per conto di terzi;
- soggetti attivi del reato sono gli Amministratori, i Direttori Generali, i Sindaci e i Liquidatori (reato proprio).

Ad esempio: l'Amministratore Delegato della società, ignorando l'indicazione del responsabile amministrativo circa l'esigenza di un accantonamento (rettifica) al Fondo svalutazione crediti a fronte della situazione di crisi di un cliente, iscrive un ammontare di crediti superiore al dovuto, al fine di non far emergere una perdita che comporterebbe l'assunzione di provvedimenti sulla riduzione del capitale sociale (artt. 2446 e 2447, c.c.).

Impedito Controllo (art. 2625 c.c.)

La condotta consiste nell'impedire o ostacolare, mediante occultamento di documenti o altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali.

Il reato, imputabile esclusivamente agli Amministratori, è punito più gravemente se la condotta ha causato un danno e la pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o comunitari o diffusi tra il pubblico in maniera rilevante ai sensi del TUF.

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

La fattispecie si concretizza con la condotta degli Amministratori che, al di fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli.

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

Il reato può essere commesso dagli Amministratori che ripartiscano utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscano riserve, anche non costituite con utili, che non possano per legge essere distribuite.

Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

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

La fattispecie di reato si concretizza quando gli Amministratori, al di fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge; ovvero quando gli Amministratori, al di fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

Il reato è estinto se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta.

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

La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di Legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o scissioni, che cagionino danno ai creditori.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Soggetti attivi del reato sono, anche in questo caso, gli Amministratori.

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

La fattispecie di reato si concretizza quando Amministratori o soci conferenti, anche in parte, formano o aumentano fittiziamente 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 di Philogen nel caso di trasformazione.

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

La fattispecie di reato si concretizza quando i Liquidatori, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, cagionano danno ai creditori.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

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

Detta fattispecie di reato è configurata al primo comma come reato proprio degli amministratori dei direttori generali dei dirigenti preposti dei sindaci e dei liquidatori della società ed il fatto tipico consiste nell'infedeltà a seguito di dazione cui consegue un procurato nocumento alla società. Il secondo comma prevede l'ipotesi residuale del medesimo fatto, punito in maniera meno grave, commesso dai sottoposti alla vigilanza dei soggetti qualificati di cui sopra.

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

La condotta tipica prevede che si determini con atti simulati o con frode la maggioranza in Assemblea, allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Il reato può essere commesso da chiunque ("reato comune"), quindi anche da soggetti esterni alla società.

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 idonee a incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

Il reato può essere commesso da chiunque ("reato comune").

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c., comma 1 e 2)

La condotta consiste nell'impedire o ostacolare l'esercizio delle funzioni di vigilanza alle autorità che le detengono per legge, con esposizioni di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria oppure occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, Deve essere un ostacolo consapevole, in qualsiasi forma, anche omettendo le comunicazioni dovute, alle funzioni delle autorità di vigilanza.

Il reato, imputabile agli organi societari di amministrazione, finanza, controllo e gli atri organi sottoposti per legge alle autorità pubbliche di vigilanza od obbligate nei loro confronti, è punito più gravemente se la condotta ha causato un danno e la pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o comunitari o diffusi tra il pubblico in maniera rilevante ai sensi del TUF.

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 e 3 D. Lgs. 74/2000)

La condotta consiste nel predisporre, utilizzando fatture o altra documentazione falsa per operazioni inesistenti, o indicando elementi passivi fittizi, una dichiarazione dei redditi o IVA non veritiera, al fine di evadere le relative imposte. E' un reato tra i più gravi fra quelli dichiarativi perchè la dichiarazione non soltanto non è veridica, ma risulta altresì insidiosa, in quanto supportata da un impianto contabile o più genericamente documentale atto a sviare od a ostacolare la successiva attività di accertamento dell'amministrazione finanziaria o comunque ad avvalorare artificiosamente l'inveritiera prospettazione di dati.

Il reato, imputabile agli organi societari di amministrazione, finanza, controllo ed a chiunque – anche esterno all'impresa - risulti coinvolto a vario titolo nella predisposizione, controllo e presentazione delle dichiarazioni, è punito con la reclusione da 4 ad 8 anni.

False fatturazioni o creazione di documenti per operazioni inesistenti (art. 8 D. Lgs. 74/2000)

La condotta consiste nel predisporre fatture o altra documentazione falsa per operazioni inesistenti, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto. E' un reato dove deve essere presente il dolo specifico, ovvero la volontà di far evadere le imposte a terzi.

Il reato, che è un reato comune, poiché può essere realizzato non solamente dal contribuente tenuto alle scritture contabili, ma anche da un soggetto estraneo a tale obbligo, è punito con la reclusione da 4 ad 8 anni.

Occultamento o distruzione di scritture contabili (art. 10 D. Lgs. 74/2000)

La condotta consiste nell'occultare o distruggere, 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, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentirne l'evasione a terzi.

Il reato, che è un reato comune, poiché può essere realizzato non solamente dal contribuente tenuto alle scritture contabili e indipendentemente dal loro concorso, ma anche da un soggetto estraneo a tale obbligo, è punito con la reclusione da 3 ad 7 anni.

Sottrazione fraudolenta al pagamento delle imposte (art. 11 D. Lgs. 74/2000)

La condotta consiste nell'alienare simulatamente, o compiere altri atti fraudolenti sui propri o su altrui beni idonei, finalizzati a rendere in tutto o in parte inefficace la procedura di riscossione coattiva delle imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte.

Il reato, che può essere compiuto solo dal contribuente, è punito con la reclusione da 6 mesi a 4 anni.

Aree a rischio

Le aree di attività considerate più specificatamente a rischio in relazione ai reati societari sono ritenute le seguenti:

- redazione del bilancio, della relazione sulla gestione, del bilancio consolidato e di altre comunicazioni sociali
- gestione della contabilità generale
- gestione rapporti con soci, Società di revisione e Collegio Sindacale
- operazioni societarie che possano incidere sull'integrità del capitale sociale
- operazioni sul capitale e destinazione dell'utile
- informative e rapporti con gli organi di informazione e stampa
- comunicazione, svolgimento e verbalizzazione Assemblee

Il rischio di commissione di reati societari in Philogen risulta comunque attenuato dal doppio controllo esterno sul bilancio esercitato dalla Società di Revisione e dal Collegio Sindacale.

Destinatari della parte speciale

Destinatari della presente parte speciale "B" sono i soggetti coinvolti nelle attività sopra menzionate (c.d. "Destinatari") ovvero:

- il CFO (Responsabile servizi finanziari) e tutta l'area Amministrazione, Finanza e Controllo
- il Consiglio di Amministrazione
- tutte le funzioni che forniscono dati ed informazioni al fine della predisposizione dei prospetti di comunicazione sociali

Principi generali di comportamento nelle aree di attività a rischio

Ai Destinatari è fatto espresso obbligo di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di Legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società e del Gruppo; pertanto è fatto divieto di:
    - predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società e del Gruppo
    - omettere di comunicare dati e informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società e del Gruppo
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di Legge e delle procedure aziendali, al fine di garantire la tutela del patrimonio degli investitori, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione ed illustrazione dei dati e delle informazioni relative ai prodotti finanziari ed agli emittenti, necessarie per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria dell'emittente e sull'evoluzione della sua attività, nonché sui prodotti finanziari e relativi diritti
- osservare tutte le norme poste dalla Legge a tutela dell'integrità ed effettività del capitale sociale e agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere; pertanto 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 (anche non costituite con utili) che non possono per legge essere distribuite
- acquistare o sottoscrivere azioni della Società fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge
- 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 fittizi del capitale sociale
- ripartire i beni sociali tra i soci – in fase di liquidazione – prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli

- assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo sulla gestione sociale previsto dalla Legge, nonché la libera e corretta formazione della volontà assembleare
- effettuare con tempestività, correttezza e completezza tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità pubbliche di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate. In ordine a tale punto, è fatto divieto di:
    - omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle Autorità in questione, tutte le comunicazioni, periodiche e non, previste dalla legge e dall'ulteriore normativa di settore, nonché la trasmissione dei dati e documenti previsti dalle norme in vigore e/o specificamente richiesti dalle predette Autorità
    - esporre in tali comunicazioni e nella documentazione trasmessa fatti non rispondenti al vero oppure occultare fatti concernenti la situazione economica, patrimoniale o finanziaria della Società e del Gruppo
    - porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle Autorità pubbliche di Vigilanza, anche in sede d'ispezione (espressa opposizione, rifiuti pretestuosi, comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti)

Procedure specifiche

Le attività amministrative e contabili, sia a livello di singola Società sia di Gruppo che risultano potenzialmente "sensibili" e che fanno riferimento in larga parte ai reati societari

sono oggetto di analisi dettagliate da parte del controllo di gestione interno, della Società di revisione e del Collegio Sindacale. Tale Sistema di Controllo Interno utilizzato dalla società Philogen fornisce tutela rispetto al rischio di commissione di reati previsti dal Decreto Legislativo 231/2001.

Nello specifico, con riferimento ai postulati di bilancio (esistenza e accadimento, completezza, valutazione e misurazione, diritti e obblighi, presentazione e informativa) e all'adeguatezza della segregazione dei compiti e ruoli, sono stati analizzati i seguenti processi aziendali (e i relativi sotto processi):

- Ciclo attivo
- Ciclo passivo
- Ciclo di magazzino
- Ciclo degli investimenti
- Cedolini e gestione del personale
- Tesoreria, cassa, banche e movimentazioni finanziarie
- Imposte e tasse
- Chiusura contabile
- Consolidamento

Pertanto, per quanto riguarda tutti gli aspetti legati alla gestione della contabilità generale e predisposizione dei progetti di bilancio civilistico, di eventuali situazioni patrimoniali in occasione dell'effettuazione di operazioni straordinarie, e altri adempimenti in materia societaria della società Philogen Spa e del Gruppo Philogen, si rimanda ai dettagliati controlli e alle valutazioni svolte dalla Società di Revisione e dal Collegio Sindacale.

Istruzioni e Verifiche dell'OdV

I compiti dell'OdV sono i seguenti:

1. per quanto riguarda il bilancio e le altre comunicazioni sociali, in ragione del fatto che il bilancio della Società è certificato da una Società di Revisione, i compiti dell'OdV si limitano a:
    a) monitoraggio dell'operato della Società di Revisione
    b) esame di eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari
    c) verifica dell'effettiva indipendenza della Società di Revisione
2. Per quanto riguarda le altre attività a rischio:
    a. verifiche periodiche sul rispetto delle procedure interne

b. esame di eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

Indicazioni finali

A completamento di quanto indicato nel presente paragrafo e per le indicazioni operative si vedano le seguenti procedure:

- “Procedura di affidamento incarichi ai Collaboratori Esterni”
- “Procedura Acquisti e Pagamenti”
- “Procedura Vendite e Incassi”
- “Procedura Gestione del Magazzino”
- “Procedura Gestione Commesse”
- “Procedura Immobilizzazioni”
- “Procedura Payroll e Gestione del Personale”
- “Procedura Tesoreria e Cassa”
- “Procedura Closing”
- “Procedura Consolidation”
- “Procedura Imposte e Tasse”

Philogen
innovating targeting

PARTE SPECIALE “C”

Reati ambientali

relativa al

Modello di Organizzazione, Gestione e Controllo

I reati ambientali

In attuazione al disposto dell'art. 1 della Legge 15 dicembre 2004, n. 308, è stato emanato il D.lgs. n. 152 del 3 aprile 2006 (di seguito il "Codice dell'Ambiente").

In alcuni casi le condotte previste dal legislatore integrano semplicemente un illecito di natura amministrativa; laddove invece sia prevista la pena dell'arresto, della reclusione, della multa o dell'ammenda, le relative fattispecie assumono rilievo penale.

Le condotte penalmente sanzionabili sono riconducibili essenzialmente a quattro categorie, ovvero:

- attività di scarico di acque reflue (art. 137, concernente gli scarichi di acque reflue industriali);
- attività di emissione in atmosfera d'impianti e attività (art. 279, concernente l'esercizio di un impianto o di un'attività in violazione dei valori limite di emissione o delle prescrizioni stabilite dall'autorizzazione ottenuta);
- attività di gestione dei rifiuti e di bonifica dei siti inquinati (artt. 255 e ss., concernenti ad esempio l'abbandono dei rifiuti, l'attività di gestione di rifiuti non autorizzata e la violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari);
- attività di combustione di materiali o sostanze diverse dai rifiuti (art. 296 concernente l'attività di combustione dei rifiuti effettuata in difformità alle prescrizioni ambientali).

Come espressamente indicato dall'art. 254 del Codice dell'Ambiente, restano comunque salve le disposizioni previste da leggi speciali.

Con la Legge 22.05.2015 n. 68 si è inteso poi effettuare un salto di qualità nella tutela della salute e dei beni naturali, introducendo nel Codice Penale un nuovo titolo, il VI bis, nel libro II, e con esso gli articoli 452 bis- 452 terdecies.

Nel titolo di cui sopra sono previste quindi le nuove fattispecie di:

- inquinamento ambientale (art. 452 bis c.p.) che consiste nella compromissione o deterioramento significativi e misurabili: 1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo; 2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna;
- disastro ambientale (art. 452 quater c.p.) costituito, al di fuori dei casi previsti dall'art. 434 c.p. alternativamente da 1) l'alterazione irreversibile dell'equilibrio di un ecosistema; 2) l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali; 3) l'offesa alla pubblica incolumità in ragione della rilevanza del fatto per l'estensione della compromissione o dei suoi effetti lesivi ovvero per il numero delle persone offese o esposte a pericolo;
- delitti colposi contro l'ambiente e quindi le ipotesi colpose dei fatti di cui ai citati articoli 452 bis e 452 quater c.p.;

- traffico e abbandono di materiale ad alta radioattività (art. 452 sexies c.p.
- impedimento di controllo (452 septies);
- omessa bonifica (452 terdecies);

Aree a rischio

Le aree di attività considerate più specificatamente a rischio riguardo ai reati ambientali sono ritenute le seguenti:

- Gestione dei rifiuti biologici
- Adempimenti normativi relativi al sistema di controllo della tracciabilità dei rifiuti speciali

Adempimenti in materia di autorizzazione agli scarichi.

Il rischio di commissione di reati ambientali in Philogen è comunque attenuato dal fatto che la gestione dei rifiuti speciali è affidata a una società esterna che si occupa di raccogliere il rifiuto speciale direttamente dal sito produttivo Philogen. Apposite procedure interne definiscono le metodologie di raccolta, consegna e tracciatura del rifiuto biologico.

È necessario altresì verificare l'affidabilità dei fornitori e delle parti terze con le quali la Società intrattiene rapporti di fornitura di tali servizi. Particolare attenzione dovrà essere data alla stipulazione di contratti e al puntuale ed effettivo svolgimento delle prestazioni concordate in conformità con le leggi vigenti.

Inoltre deve essere prestata particolare attenzione a tutti gli adempimenti autorizzativi in materia di scarichi di varia natura nel rispetto della normativa vigente sia nazionale che locale.

Destinatari della parte speciale

Destinatari della presente parte speciale "C" sono i soggetti coinvolti nelle attività sopra menzionate (c.d. "Destinatari") ovvero:

- il responsabile della produzione
- il Consiglio di Amministrazione
- tutte le funzioni che forniscono dati ed informazioni necessarie al corretto smaltimento dei rifiuti.

Principi generali di comportamento nelle aree di attività a rischio

Nell'espletamento delle rispettive attività/funzioni, oltre a quanto contenuto nel modello, i soggetti destinatari sono tenuti a:

- astenersi dal porre in essere comportamenti tali da integrare i reati di abbandono e deposito incontrollato di rifiuti sul suolo e nel suolo
- astenersi dal porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato rientranti tra quelle di cui sopra, possano potenzialmente diventarlo
- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto di norme di legge e regolamenti e delle procedure interne aziendali

In particolare sono vietati i seguenti comportamenti:

- l'abbandono e il deposito incontrollati di rifiuti sul suolo e nel suolo
- l'immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee

A tutti i destinatari è fatta espressa richiesta di:

- seguire le procedure interne relative al corretto stoccaggio e smaltimento dei rifiuti biologici;
- segnalare tempestivamente al proprio responsabile qualunque violazione in tale ambito eseguita da tutti i prestatori di servizio esterni alla società.

Istruzioni e Verifiche dell'OdV

I compiti dell'OdV sono in generale verificare la corretta tracciabilità delle fasi del processo di smaltimento del rifiuto biologico.

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

- tracciabilità delle singole attività (documentazione a supporto)
- verifica della corrispondenza delle dichiarazioni/certificazioni presentate con la

documentazione tecnica di supporto

- verifica della corretta attuazione delle procedure definite.

Per quanto riguarda le altre attività a rischio:

- verifiche periodiche sul rispetto delle procedure interne

- esame di eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari

Indicazioni finali

A completamento di quanto indicato nel presente paragrafo e per le indicazioni operative si faccia riferimento alla seguente procedura:

- “Procedura di smaltimento dei rifiuti”

Philogen
innovating targeting

PARTE SPECIALE “D”

Reati connessi alla sicurezza del lavoro

relativa al

Modello di Organizzazione, Gestione e Controllo

Reati connessi alla sicurezza sul lavoro

La Legge 3 agosto 2007, n. 123 è intervenuta inserendo nel Decreto l'art. 25-septies, poi modificato dall'art. 300 comma 1 d.lgs. 9 aprile 2008 n. 81, disposizione che estende il regime della responsabilità amministrativa delle persone giuridiche alle ipotesi di omicidio colposo e lesioni colpose gravi o gravissime (articoli 589 e 590, co. 3 c.p.) commessi con violazione delle norme antinfortunistiche e sulla tutela della salute sul lavoro.

La più evidente modifica prevede un'articolata modulazione delle sanzioni a carico dell'Ente, secondo una triplice distinzione:

1. per il delitto di omicidio colposo commesso con violazione dell'art. 55, comma 2, T.U. (omessa o parzialmente incompleta valutazione dei rischi relativamente alle aziende ivi contemplate), la sanzione è pari a 1.000 quote, oltre a sanzioni interdittive da tre mesi a un anno;
2. per il delitto di omicidio colposo commesso con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro (diverse da quella sopra indicata), si applica la sanzione da 250 a 500 quote, oltre a sanzioni interdittive da tre mesi a un anno;
3. per il delitto di lesioni gravi o gravissime colpose commesso con violazione delle norme sulla tutela e sulla sicurezza sul lavoro, una sanzione non maggiore a 250 quote, oltre a sanzioni interdittive fino a sei mesi.

La punibilità degli enti riguarda sia i delitti perseguibili a titolo doloso (coscienza e volontarietà dell'azione criminosa) che i delitti colposi (mancanza di volontarietà nella realizzazione dell'evento giuridico rilevante).

Le sanzioni previste dal Decreto potranno essere applicate esclusivamente qualora gli stessi siano stati commessi nell'interesse o a vantaggio dell'ente (anche potenziale), ovvero quando la violazione delle norme antinfortunistiche sia finalizzata a un risparmio economico o anche semplicemente di tempo per la Società.

Omicidio colposo (art. 589 c.p.)

Il reato si configura quando chiunque cagiona per colpa la morte di una persona. Nel caso di morte di una o più persone e di lesioni di una o più persone è applicata la pena che dovrebbe infliggersi per la più grave delle violazioni commesse.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui, a seguito della violazione di una delle norme antinfortunistiche come ad esempio l'utilizzo dei dispositivi di protezione individuale (DPI), si verificasse un evento mortale.

Lesioni personali colpose (art. 590 c.p.)

Il reato si configura quando chiunque cagiona per colpa una lesione personale. Nel caso di lesioni di una o più persone è applicata la pena che dovrebbe infliggersi per la più grave delle violazioni commesse.

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

- dal fatto deriva una malattia che mette in pericolo la vita della persona offesa, oppure una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;
- 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, oppure la perdita dell'uso di un organo o della capacità di procreare, oppure una permanente e grave difficoltà del linguaggio;
- la deformazione, oppure lo sfregio permanente del viso.

Come in precedenza affermato, nel novero dei reati previsti dal D.lgs. 231/01 rientrano le fattispecie di lesioni personali colpose gravi e gravissime.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui, a seguito della violazione di una delle norme antinfortunistiche come ad esempio l'utilizzo dei dispositivi di protezione individuale (DPI), si verificasse un incidente con prognosi superiore ai quaranta giorni.

Aree a rischio

Le aree e le attività operative maggiormente esposte a rischio riguardo ai reati connessi alla sicurezza, sono le stesse aree per le quali la Società, attraverso il proprio sistema di gestione della sicurezza, si è già adeguata alle previsioni normative del D.lgs. n. 81 del 9 aprile 2008.

In particolare, come previsto dal Decreto, Philogen ha valutato i rischi per la sicurezza e la salute dei lavoratori aziendali, ivi compresi quelli riguardanti i gruppi di lavoratori esposti a rischi particolari e i collaboratori esterni.

Le evidenze raccolte e il programma di miglioramento sono esposti nel Documento di Valutazione dei Rischi in vigore alla data di emissione della presente Parte Speciale che permette di tenere traccia dell'attività di prevenzione e controllo nel campo della sicurezza

e dell'igiene nei luoghi di lavoro nonché di valutare il livello di rischio residuo presente all'interno dell'azienda.

Da questa indagine vengono quindi periodicamente individuate le aree / attività / mansioni aziendali che possono potenzialmente configurare un rischio per la salute e la sicurezza del dipendente Philogen. In particolare il Documento di Valutazione dei Rischi di Philogen definisce i settori e/o i processi aziendali che potenzialmente possono incorrere nei reati previsti dal d.lgs. 231/01 ed elencati nella presente Parte Speciale.

Per ciascun'area a rischio-reato sono quindi analizzati i soggetti interni coinvolti e i 'protocolli' di controllo adottati dall'azienda per evitare che tali reati possano effettivamente verificarsi.

In definitiva dai contenuti del Documento di Valutazione dei Rischi di Philogen è possibile rilevare che tutte le attività aziendali hanno valori di rischio residuo accettabile, tenuto conto della specificità del lavoro caratterizzato da attività di ufficio e attività esterna.

I rischi lavorativi possono essere divisi in tre categorie:

- Rischi per la Sicurezza (di natura infortunistica)
- Rischi per la Salute (di natura igienico ambientale)
- Rischi organizzativi (condizioni di lavoro difficili)

Rischi per la sicurezza

Sono quelli responsabili del potenziale verificarsi d'incidenti o infortuni, subite dagli operatori, in conseguenza di un impatto fisico-traumatico di diversa natura (meccanica, elettrica, chimica, termica ecc.).

Rischi per la salute

Sono quelli che comportano l'emissione nell'ambiente di fattori ambientali di rischio, di natura chimica fisica e biologica, con conseguente esposizione del personale addetto.

Rischi organizzativi

Sono quelli concernenti lavori usuranti e dovuti a condizioni di lavoro difficili.

Il Documento di Valutazione dei Rischi analizza i tre tipi di rischi per ogni reparto e settore dell'Officina Farmaceutica Philogen in modo da consentire al Datore di Lavoro di:

1. Individuare i provvedimenti urgenti da attuare per proteggere la sicurezza e salute dei dipendenti e degli altri lavoratori
2. Migliorare il livello di protezione dei lavoratori, rispetto alle esigenze della sicurezza
3. Informare e formare i lavoratori
4. Organizzare i mezzi destinati alla prevenzione.

Destinatari della parte speciale

I reati elencati nella presente Parte Speciale si riferiscono a comportamenti posti in essere da Amministratori, Dirigenti e Dipendenti di Philogen nelle aree di attività a rischio, nonché dai Collaboratori esterni e i Partner, così come già definiti nella Parte Generale del Modello di Organizzazione, Gestione e Controllo.

Tutti i destinatari della presente Parte Speciale devono dunque rispettare comportamenti conformi a quanto di seguito formulato, al fine di impedire il verificarsi dei reati previsti.

I principi generali di comportamento

I soggetti destinatari della presente Parte Speciale (elencati al precedente paragrafo) coinvolti nelle attività definite "a rischio" devono rispettare principi e norme di comportamento di seguito dettate, nel rispetto degli obblighi normativi, delle procedure aziendali e del Codice Etico di Philogen.

È assolutamente vietato:

- mettere in atto comportamenti tali da esporre l'azienda ad una delle fattispecie di reato previste dall'art. 25 - septies del D.Lgs. 231/2001;
- mettere in atto comportamenti tali da favorire l'attuarsi di fattispecie di reato previste dall'art. 25 - septies del d.lgs. 231/2001;
- omettere l'aggiornamento delle misure di prevenzione, in relazione a mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e della sicurezza del lavoro, ovvero in relazione al grado di evoluzione della tecnica, della prevenzione e della protezione;
- omettere la fornitura ai lavoratori dei mezzi personali di protezione;
- omettere l'adozione di misure appropriate affinché soltanto i lavoratori che abbiano ricevuto adeguate istruzioni possano accedere nelle zone che li espongono ad un rischio grave e specifico;
- emanare ordini di ripresa del lavoro, nonostante la persistenza di una situazione di pericolo grave ed immediato;

- omettere l'adozione di provvedimenti idonei ad evitare che le misure tecniche impiegate possano causare rischi per la salute della popolazione e danni all'ambiente esterno;
- omettere l'adozione di misure antincendio e di pronta evacuazione in caso di pericolo grave e immediato.

Per tutto ciò è necessario il rispetto dei seguenti principi:

1. rispettare le prescrizioni contenute nel Codice Etico di Philogen;
2. rispettare le prescrizioni impartite dalla segnaletica di sicurezza nonché i contenuti delle procedure di sicurezza/emergenza trasmesse anche attraverso la formazione di aula;
3. rispettare le procedure di sicurezza/emergenza trasmesse dal RSPP a ogni singolo collaboratore, anche esterno, all'Azienda.

Procedure specifiche

L'ambito della tutela della salute e della sicurezza del lavoro è già ampiamente normato (D.lgs. 81/2008 e successive modifiche e integrazioni) e l'adeguamento alle previsioni normative viene oggi assolto dal responsabile del servizio di prevenzione e protezione (RSPP) durante il lavoro, interno o esterno all'azienda.

Nell'ottica di un'armonizzazione tra quanto già fatto nell'ambito della prevenzione degli infortuni sul lavoro e quanto è invece previsto dal D.lgs. 231/01, la Società deve fare in modo che si dia piena attuazione alle procedure già inserite nel piano della sicurezza dai rischi professionali e della prevenzione degli infortuni sul lavoro.

Il Responsabile Interno per le aree a rischio

L'Azienda e nello specifico il Datore di Lavoro, al fine di assolvere gli obblighi normativi, ha nominato:

- il Responsabile del Servizio di Prevenzione e Protezione (RSPP) nella persona del Dott. Tiziano Scalacci
- il Medico Competente Aziendale (MC) nella persona del Dott. Massimo Chezzi.
- il Rappresentante dei lavoratori nella persona di Michele Rosi.

Il Datore di Lavoro presiede le attività aziendali e garantisce il mantenimento e il miglioramento delle condizioni di sicurezza e igiene sui luoghi di lavoro e la manutenzione dei sistemi di prevenzione degli infortuni/incidenti.

Il medico collabora con il RSPP e con il Rappresentante dei lavoratori per tutti gli aspetti legati alla salute e alla sicurezza dei dipendenti Philogen.

Il medico competente monitorizza lo stato di salute dei lavoratori potenzialmente a rischio mediante l'esecuzione di due visite mediche l'anno.

Il RSPP redige, in collaborazione con il Datore di Lavoro e il MC il Documento di valutazione dei Rischi di Philogen per dare evidenza in modo corretto e adeguato delle attività lavorative svolte all'interno dell'Azienda e le eventuali mansioni a rischio ivi compreso un programma di miglioramento teso a eliminare o ridurre i rischi.

Istruzioni e Verifiche dell'OdV

I compiti dell'OdV sono in generale verificare la corretta attuazione di quanto previsto dal D.lgs. 81/2008 e in particolare:

- verifica dell'osservanza, dell'attuazione e dell'adeguatezza del Modello (Parte Generale e Parti Speciali) in ottica di prevenzione della commissione dei reati contro la persona;
- verifica della corretta redazione e aggiornamento del Documento Unico di Valutazione dei Rischi (DVR);
- predisposizione di adeguati flussi informativi in merito agli infortuni occorsi;
- verifica dell'attività di controllo effettuata dai delegati del datore di lavoro in particolare delle figure di RSPP e MC;
- predisposizione di un programma di audit sulla corretta attuazione delle procedure per la prevenzione degli infortuni;
- verifica della corretta attuazione del programma di formazione in materia di salute e sicurezza.

L'OdV comunica i risultati della propria attività di vigilanza e controllo al Consiglio di Amministrazione e al Collegio Sindacale, secondo i termini indicati nel Regolamento dell'OdV e nella Parte Generale del Modello.

Indicazioni Finali

A completamento di quanto indicato nel presente paragrafo e per le indicazioni operative si vedano i seguenti documenti:

- "Regolamento dell'OdV"
- "Documento di Valutazione dei Rischi di Philogen"

- “Gestione della Prevenzione per la Salute e Sicurezza”
- “Controllo lava occhi e doccia”
- “Controllo e gestione cassette pronto soccorso”
- “Addestramento del Personale”

Philogen
innovating targeting

PARTE SPECIALE “E”

Reati informatici e il trattamento illecito di dati

relativa al

Modello di Organizzazione, Gestione e Controllo

Disciplinare interno per il personale dipendente

E.1. I reati informatici e il trattamento illecito di dati

L'articolo 7, Legge n. 48 del 18 marzo 2008 ("Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno" pubblicata sulla Gazzetta Ufficiale n. 80 del 4 aprile 2008) ha modificato il D.Lgs. 231/2001 inserendo tra i reati-presupposto i reati informatici, e conseguenti a trattamento illecito di dati.

In particolare, la legge ha introdotto nel Decreto 231 l'art. 24 bis il quale dispone:

1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a

quattrocento quote.

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

La disposizione in esame:

- recepisce tra i Reati l'art. 491-bis c.p. che, a sua volta, estende le ipotesi di falsità in atti di cui al Libro II, Titolo VII, Capo III c.p. a tutte le fattispecie delittuose in cui una o più delle suddette falsità abbiano ad oggetto un cd. "documento informatico";

• introduce all'interno del D.Lgs. 231/2001 alcune ipotesi di reato in materia di criminalità informatica, in parte già disciplinate dal codice penale.

Prima della ratifica della Convenzione di Budapest, il D.Lgs. 231/2001 conosceva, quale reato c.d. informatico, presupposto per la responsabilità dell'ente, unicamente la fattispecie descritta dall'art. 640- ter del codice penale (frode informatica), qualora commessa "…in danno dello Stato o di un Ente Pubblico" (art. 24).

Motivo di tale integrazione normativa è da ravvisarsi nell'esigenza di introdurre forme di responsabilità per le persone giuridiche, in riferimento alla commissione di alcuni dei reati informatici più gravi, anche nel caso in cui soggetto passivo non sia una Pubblica Amministrazione.

Le fattispecie inerenti i reati descritti nella presente Sezione della Parte Speciale sono state introdotte per la prima volta nel codice penale con l'approvazione della Legge n. 547/1993 (con specifico riferimento agli articoli 3, 4, 6 e 9).

Da ultimo, proprio la Legge n. 48/2008, nell'inserire le predette fattispecie nel novero dei Reati presupposto, ha provveduto, da una parte, a modificare gli articoli 615-quinquies e 635-bis c.p. e, dall'altra, ad introdurre nuove fattispecie in materia, quali quelle previste dall'articolo 640-quinquies c.p. e dagli articoli 635-ter e 635-quater.

Di seguito si riportano le norme contenute nel codice penale disciplinanti i reati individuati.

Art. 491-bis c.p. Documenti informatici

Se alcuna delle falsità previste dal presente capo [(si tratta del Capo III ("Della falsità in atti") del Titolo VII ("Dei delitti contro la fede pubblica") del Libro II del codice penale)] riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.

Con riferimento all'art. 491-bis c.p. occorre precisare che per "documento informatico" deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, 1° co., lett. p, D.Lgs. n. 82 del 2005 "Codice dell'Amministrazione Digitale").

In seguito alla novella, la definizione si sostituisce a quella precedentemente disciplinata dall'art. 491- bis c.p., secondo periodo, c.p., il quale stabiliva che: "per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".

Separando la nozione di “documento” da quella di “supporto”, si è determinata una maggiore chiarezza concettuale, in quanto l’assimilazione tra documento e supporto rischiava di attribuire al documento informatico una illusoria dimensione materiale dalla quale esso, in realtà, prescindeva.

In merito all’efficacia probatoria (art. 21 del “codice dell’amministrazione digitale”) che il documento informatico deve possedere per essere ritenuto tale, va sottolineato che:

- esso deve essere sottoscritto con firma elettronica potendo, in caso contrario, soddisfare al più il requisito legale della forma scritta, a discrezione del giudice;

- anche quando è munito di una firma elettronica “semplice” (cioè non qualificata), potrebbe non avere efficacia probatoria, dipendendo tale effetto dalla decisione assunta dal giudice nel singolo caso concreto, una volta valutati parametri quali ad esempio le caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità del documento informatico.

Pertanto, nel caso in cui il documento informatico non possieda alcuna efficacia probatoria non si configureranno le fattispecie delittuose indicate nel ricordato Capo III del codice penale.

Risulta di fondamentale importanza, per meglio comprendere la categoria dei reati di falso, conoscere la distinzione tra “falso materiale” e “falso ideologico”.

I concetti fanno leva sulle nozioni di “genuinità” e “veridicità” del documento in base alle quali:

- un documento è “genuino” se sussiste concordanza tra l’autore reale e l’autore apparente e se, una volta formato in via definitiva, non ha subito alterazioni;

- un documento è “veridico” se, oltre ad essere genuino perchè compilato dall’autore apparente, attesta dati conformi al vero.

Pertanto:

- il “falso materiale” si verifica in presenza di una condotta che esclude la genuinità dell’atto (ad esempio perché quest’ultimo è stato contraffatto, ossia redatto da persona diversa da quella all’apparenza autrice, ovvero alterato, vale a dire modificato in epoca successiva rispetto alla sua definitiva formazione);

- il “falso ideologico” si verifica allorquando un documento attesta fatti non conformi al vero.

Si esaminano di seguito singole fattispecie: REATI INFORMATICI.

La Legge n. 48/2008 assolve nel nostro ordinamento all'esigenza di riordino ed armonizzazione tra gli

Stati membri dell'Unione Europea dei cd. "Computer Crimes".

In particolare, l'articolato prevede l'introduzione di nuove norme incriminatrici e l'aggravamento di alcune fattispecie già esistenti, oltre ad introdurre elementi procedurali utili al perseguimento dei reati.

I reati informatici recepiti all'interno del nuovo art. 24 bis del D.Lgs. 231/2001 sono i seguenti:

Art. 615-ter c.p. Accesso abusivo ad un sistema informatico o telematico

1. Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

2. La pena è della reclusione da uno a cinque anni:

• se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

• se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

• se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

3. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

4. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Art. 615-quater c.p. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

1. Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico,

protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

2. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

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

1. Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

Art. 617-quater c.p. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

1. Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

2. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

3. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

4. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è 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 necessità;
- da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- da chi esercita anche abusivamente la professione di investigatore privato.

Art. 617-quinquies c.p. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

1. Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

2. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617- quater.

Art. 635-bis c.p. Danneggiamento di informazioni, dati e programmi informatici

1. Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

2. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

Art. 635-ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo

Stato o da altro ente pubblico, o comunque di pubblica utilità

1. Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

2. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

3 Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Art.635-quater c.p. Danneggiamento di sistemi informatici o telematici

1. Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635- bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni

o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola

gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

2. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Art. 635-quinquies c.p. Danneggiamento di sistemi informatici o telematici di pubblica utilità

1. Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

2. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

3 Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Art. 640-quinquies c.p. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

Si commentano di seguito le fattispecie sopra riportate:

Le ipotesi delittuose attinenti l'indebito utilizzo di apparecchiature e sistemi informatici rientrano in alcuni casi tra i delitti contro l'inviolabilità del domicilio, e in altri tra quelli contro l'inviolabilità dei segreti, rispettivamente Sezioni IV e V del Capo III ("Dei delitti contro la libertà individuale") del Titolo XII ("Dei delitti contro la persona") del Libro II del codice penale.

In altri casi ancora si tratta di delitti contro il patrimonio (Titolo XIII del libro II), alcuni dei quali si concretizzano in atti di violenza sulle cose (Capo I), altri in atti di frode (Capo II).

Sono ricompresi tra i delitti contro l'inviolabilità del domicilio:

- l'accesso abusivo a un sistema informatico (615-ter c.p.);
- la detenzione o diffusione abusiva di codici di accesso a sistemi (615-quater c.p.);
- la diffusione di programmi diretti a danneggiare o interrompere il sistema (615-quinquies c.p.).

Con la previsione di tali delitti il Legislatore ha voluto garantire la protezione del "domicilio informatico" quale spazio ideale (ma anche fisico, in cui sono contenuti i dati informatici) di pertinenza della sfera individuale, quale bene costituzionalmente protetto.

E' comprensibile di conseguenza, che la fattispecie di cui all'art. 615-ter c.p. presenti elementi costitutivi comuni alla violazione di domicilio (artt. 614 c.p. e 615 c.p.). Elemento fondamentale è la volontà tacita o espressa contraria all'accesso abusivo da parte di chi ha il cosiddetto ius excludendi alios.

Inoltre anche nelle fattispecie in esame le condotte punite sono di due tipi:

- introduzione nel sistema;
- permanenza in esso.

La manifestazione di volontà, da parte dell'avente diritto, di escludere chi si vuole introdurre (o chi si è introdotto, e si trattiene indebitamente) può essere sia manifesta sia tacita.

Particolarmente interessante è che all'introduzione violenta (vale a dire contraria alla volontà del proprietario) è equiparata quella clandestina (vale a dire posta in essere di nascosto).

Si tratta di elementi costitutivi della violazione di domicilio, rintracciabili anche nella fattispecie di cui all'art. 615-ter c.p.

I delitti di cui agli artt. 615-quater c.p. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, e 615-quinquies c.p. - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, presentano invece elementi diversi.

Il delitto di cui all'art. 615-quater c.p. è un reato di pericolo. La condotta in esso prevista, infatti, non è di per sé dannosa, né è causalmente orientata alla produzione di un evento dannoso. Essa è punita al fine di evitare la consumazione di più gravi delitti come per esempio quelli di accesso abusivo a sistema informatico, o di frode informatica ai danni dello Stato o di altro ente pubblico.

Entrambe le fattispecie richiedono il dolo specifico. Esso consiste nel primo caso nel fine di procurare all'agente o ad altri un profitto ovvero di arrecare ad altri un danno, mentre nel secondo caso nello scopo di danneggiare illecitamente un sistema informatico o telematico.

Alcuni esempi di condotte punibili sulla base delle norme incriminatrici ora considerate sono:

- superare, attraverso il ricorso ad un accorgimento tecnico, il blocco di un centralino e riuscire così a effettuare telefonate a cui l'utenza non è abilitata, accedendo così abusivamente alla linea telefonica (art. 615-ter c.p.);
- procurarsi il numero seriale di un apparecchio cellulare al fine di utilizzarlo congiuntamente a una scheda clonata (art. 615-quater c.p.);
- diffondere un programma contenente virus finalizzati al danneggiamento del sistema informatico o telematico (art. 615-quinquies c.p.).

Rientrano tra i delitti contro l'inviolabilità dei segreti l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617-quater c.p.) e l'installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (617-quinquies c.p.).

Con la previsione di tali delitti il legislatore ha rivisitato la protezione delle comunicazioni e della corrispondenza in funzione dello sviluppo tecnologico.

La fattispecie prevista dall'art. 617-quater c.p. punisce due differenti modalità di commissione del reato. La prima modalità è quella delle condotte previste dal comma 1, cioè di chi in modo fraudolento intercetti le comunicazioni relative a un sistema informatico o telematico oppure le ostacoli od interrompa. La commissione di tali condotte rende sempre necessario un intervento dell'agente sulla rete, con cui pertanto egli interagisce.

La disposizione di cui al comma 2, invece, punisce la rivelazione delle comunicazioni di cui al primo comma. Si tratta di condotta assolutamente differente, che può essere commessa anche da persona che non ha avuto alcuna interazione con la rete violata e che è semplicemente entrata in possesso delle comunicazioni protette.

Vi è poi una clausola di riserva, con cui si prevede la punibilità della condotta sulla base dell'art. 617-quater comma 2, salvo che il fatto non costituisca più grave reato.

Per esempio, nel caso in cui la rivelazione della comunicazioni integri le ipotesi di rivelazione di un segreto di ufficio (art. 326 c.p.), il fatto sarà punito sulla base di quella norma incriminatrice e non dell'art. 617-quater c.p.

Sono delitti contro il patrimonio mediante violenza sulle cose le fattispecie di danneggiamento di informazioni, dati e programmi informatici, e danneggiamento di sistemi informatici o telematici, di cui agli artt. 635-bis c.p., 635-ter c.p., 635- quater c.p. e 635-quinquies c.p.

Si tratta di fattispecie che presentano elementi costitutivi comuni al delitto di danneggiamento "comune", punito dall'art 635 c.p.

Anche con riferimento a tali fattispecie, infatti, si prevedono una pluralità di condotte di vario tipo: danneggiamento, deterioramento, cancellazione, alterazione, rendere inservibili i beni a cui fanno riferimento le varie norme incriminatrici.

Anche dal punto di vista dello scopo della tutela penale, si ravvisa la completa sovrapponibilità delle fattispecie in esame con quella del delitto di danneggiamento, consistendo tale scopo nel mantenimento dell'integrità del patrimonio. Le condotte punite, infatti, non implicano alcun trapasso dei beni dal patrimonio della persona offesa a quello dell'agente, bensì soltanto un peggioramento della situazione patrimoniale della persona offesa.

Le due norme di cui agli artt. 635-bis c.p. e 635-quater c.p. contengono una clausola di riserva espressa, secondo la quale esse sono applicabili salvo che il fatto costituisca più grave reato.

La clausola di riserva deve essere riferita innanzi tutto alle ipotesi di danneggiamento di informazioni, dati e programmi o sistemi informatici / telematici di pubblica utilità (635-ter e 635-quinquies), con cui i meno gravi delitti di cui agli artt. 635-bis c.p. e 635-quater c.p. sono rispettivamente in rapporto di sussidiarietà.

Le fattispecie di cui agli artt. 635-ter c.p. e 635-quinquies c.p., inoltre, prevedono un'anticipazione del momento consumativo del reato. Si prevede, infatti, che siano puniti i fatti diretti al danneggiamento, nelle varie forme e modalità di cui si è detto sopra, anche se dal fatto non deriva concretamente un danneggiamento vero e proprio. Tale ultimo caso costituisce soltanto una circostanza aggravante del reato.

Proprio per quanto si è detto, pare potersi ricomprendere tali fattispecie tra i reati di attentato o cd. "a consumazione anticipata".

Si tratta di figure incompatibili con il delitto tentato perché in tali casi il tentativo equivale già alla consumazione del reato.

Inoltre, per tutti i delitti considerati (artt. 635-bis c.p., 635-ter c.p., 635-quater c.p. E 635-quinquies c.p.) vi è un aggravamento di pena qualora ricorra la circostanza di cui all'art. 635 comma 2 n. 1 c.p. (fatto commesso con violenza alla persona o con minaccia), oppure qualora l'agente commetta il fatto con abuso della qualità di operatore del sistema.

Quanto alla fattispecie di cui all'art. 640-quinquies c.p., si tratta di un delitto contro il patrimonio mediante frode.

Anche tale ipotesi di reato è stata introdotta dalla Legge n. 48/2008. Il contenuto della condotta punita consiste nella violazione di obblighi previsti da altra legge (quelli imposti per il rilascio di certificato di firma elettronica).

Il dolo è specifico e consiste nel fine di procurare all'agente o ad altri un ingiusto profitto ovvero di arrecare ad altri danno.

Si tratta di un reato proprio. Infatti, la condotta è punita soltanto quando essa è commessa da un particolare soggetto, cioè colui che "presta servizi di certificazione elettronica". Occorre precisare che Philogen non presta servizi di certificazione elettronica e quindi la commissione di quest'ultimo reato non è ipotizzabile. Ciò nonostante per completezza si è voluto illustrarlo nella Parte Generale.

Quanto alle altre fattispecie occorre evidenziare che l'utilizzo degli strumenti informatici è riservato solo a una parte del personale (amministratori e impiegati). Di conseguenza la possibilità che si realizzino le condotte criminose sopra illustrate, risulta circoscritta a specifiche mansioni.

E.2. Scopi della Parte Speciale

Il presente capitolo della Parte Speciale si riferisce a comportamenti posti in essere dagli amministratori e dai dipendenti di Philogen, nonchè dai suoi consulenti e partners.

Nell'ambito dei Processi Sensibili tutti i destinatari del Modello, come sopra individuati, debbono adottare regole di condotta conformi a quanto prescritto dal Modello stesso al fine di prevenire il verificarsi dei reati considerati in questa Sezione.

Nello specifico, la presente Sezione della Parte Speciale ha lo scopo di:

a) indicare le procedure che i dipendenti, i consulenti e partners di Philogen sono tenuti ad osservare ai fini della corretta applicazione del Modello;

b) fornire ai responsabili gli strumenti esecutivi per esercitare le necessarie attività di controllo, monitoraggio e verifica.

E.3. Processi Sensibili nell'ambito dei delitti informatici e del trattamento illecito di dati

All'esito dell'attività di individuazione delle aree a rischio di commissione reati, svolta ai sensi dell'art. 6, comma 1, lett. a) del D.Lgs. 231/2001, sono emersi i seguenti processi sensibili rilevanti in relazione ai Reati di cui alla presente Sezione della Parte Speciale.

Essi riguardano principalmente:

• l'accesso al sistema informatico interno ed esterno (internet) da parte degli amministratori e dei dipendenti, consulenti e partners di Philogen nell'esercizio delle mansioni loro assegnate;

• l'accesso a sistemi informatici e banche dati di proprietà di terzi, con particolare riferimento a sistemi e banche dati di enti pubblici;

• l'utilizzo delle password, dei codici d'accesso, e delle (eventuali) smart card personali, nonché l'utilizzo e la conservazione di password, codici, e di qualunque altro dato o informazione utili a consentire l'accesso e/o la permanenza in un sistema informatico o telematico;

• l'utilizzo della posta elettronica;

• l'accesso, l'utilizzo ed il salvataggio di informazioni aziendali rilevanti.

Più in particolare, dunque, i processi sensibili riguardano gli ambiti specificamente previsti e regolati dalle procedure e linee guida interne, e dunque, a titolo esemplificativo e non esaustivo:

a) l'utilizzo della connessione ad internet, e quindi la consultazione e navigazione, lo streaming ed il

downloading;

b) più nel dettaglio, le operazioni di accesso a sistemi informatici e banche dati che siano dotate di sistemi di protezione e/o di restrizioni all'accesso, con particolare riferimento alla preventiva verifica della titolarità del diritto di accesso, alle modalità di accesso, ed all'utilizzo, conservazione e tutela di eventuali password, codici, e di qualunque altro dato o informazione utili a consentire l'accesso e/o la permanenza a detti sistemi informatici o telematici;

c) le modalità di utilizzo delle postazioni telematiche aziendali singolarmente assegnate;

d) l'invio o la memorizzazione di dati, in generale, e di informazioni riservate (ad esempio username e

password, PIN e PUK della smart card) in particolare;

e) l'utilizzo e la condivisione sul sistema informatico di dati personali identificativi del singolo utente;

f) l'utilizzo ovvero la modifica a vario titolo, anche se autorizzata, di software ed hardware fornito dall'azienda;

g) l'utilizzo esterno ed interno della posta elettronica aziendale, nonché della casella singolarmente

riferibile all'utente;

h) l'attività di designazione delle credenziali di autorizzazione (username, password e smart card) ad ogni singolo collaboratore o dipendente che sia chiamato ad utilizzare gli strumenti informatici aziendali.

In termini più generali, l'intera attività inerente l'utilizzo del sistema informatico aziendale, sia per ciò che concerne la connessione all'esterno, sia per quanto riferibile al c.d. sistema "intranet", può assumere carattere sensibile in ordine al rischio di commissione dei Reati di cui alla presente Sezione, dal momento che proprio la salvaguardia dei sistemi dall'accesso abusivo di terzi non autorizzati, e la regolamentazione ed il controllo dell'utilizzo degli strumenti informatici aziendali, ha costituito uno degli aspetti più delicati e dibattuti rispettivamente della criminologia informatica e della normativa sul lavoro in materia di controllo del dipendente.

Tutto ciò costituisce parte di una cultura inerente la sicurezza aziendale che, evidentemente, ci si impone di perseguire anche attraverso l'adozione del Modello, e prima ancora delle procedure specifiche che la Società ha implementato nel corso degli anni.

E.4. Regole generali

Nella presente Sezione si delineano gli specifici obblighi che devono essere rispettati dai componenti degli amministratori, dipendenti, consulenti e partners, in riferimento alla normativa sulla lotta ai reati informatici.

I soggetti summenzionati devono conoscere e rispettare:

- il Codice Etico,
- la struttura gerarchico-funzionale aziendale,
- il Regolamento interno per l'utilizzo degli strumenti Informatici (da aggiornarsi periodicamente quando necessario);
- i principi fondamentali della Normativa sulla Privacy (GDPR 679/2016; D.Lgs. 196/03 e s.m.i.)
- le caratteristiche dell'incarico di amministratore di sistema;

- le istruzioni per il personale;

- le altre eventuali disposizioni organizzative emanate dalla Società al fine di stabilire policies aziendali coerenti ed uniformi.

Le misure generali per la prevenzione dei reati informatici poste a presidio di attività finalizzate al trattamento illecito di dati, sono inoltre:

• la previsione di idonee procedure per l'assegnazione e la gestione di credenziali di autenticazione personali (username, password e smart card) e la determinazione di coerenti termini di validità delle medesime;

• la previsione di idonee procedure per la conseguente profilazione degli utenti e il loro accesso autorizzato agli strumenti informatici; cioè il conferimento a dipendenti, consulenti e partners delle credenziali di accesso alle diverse sezioni del sistema informatico aziendale, ed in genere a dati, informazioni, sistemi informatici e telematici cui la Società abbia accesso, nei limiti in cui tale accesso sia funzionale allo svolgimento del relativo incarico, e coerente agli obiettivi aziendali;

• la responsabilizzazione di ogni singolo utente riguardo ad eventuali anomalie in relazione alle attività di salvataggio automatico e memorizzazione di dati, nell'ambito dei più ampi presidi posti dalla società a tutela della sicurezza, della integrità, e della riservatezza dei dati;

• l'utilizzo della posta elettronica aziendale per ragioni (di norma) giustificate da esigenze di servizio ed, in ogni caso, il divieto esplicito di trasmissione attraverso tale strumento di:

- materiale di proprietà della Società e/o confidenziale qualora i destinatari siano indirizzi non definiti e riconosciuti dal sistema aziendale;

- mail contenenti messaggi anonimi e/o lettere a catena;

- mail contenenti credenziali di autorizzazione personali (username e password, PIN e PUK della smart card) ovvero l'indirizzo di posta elettronica personale, in caso di comunicazioni al di fuori della realtà aziendale non motivate da ragioni di servizio;

- comunicazioni finalizzate all'iscrizione a "newsletter" sospette;

• l'utilizzo della connessione ad Internet per ragioni (di norma) giustificate di servizio e di carattere professionale;

• in ogni caso l'espresso divieto, salvo autorizzazioni particolari comprovate da ragioni di servizio, di connessione, e conseguente consultazione, navigazione, streaming ed estrazione mediante downloading, a siti web che siano da considerarsi illeciti alla luce delle disposizioni organizzative interne in argomento (e quindi, a titolo esemplificativo, siti che presentino contenuti contrari alla morale, alla libertà di culto ed all'ordine pubblico, che consentano violazione della privacy di persone fisiche e giuridiche,

che promuovano o appoggino movimenti terroristici o sovversivi, riconducibili ad attività di pirateria informatica, ovvero che violino le norme dettate in materia di copyright e di proprietà intellettuale);

• la previsione del divieto di modifica delle configurazioni standard di software ed hardware aziendale;

• l'espresso divieto di aggirare le regole di sicurezza imposte sugli strumenti informatici aziendali e sulle reti di collegamento interne ed esterne;

• l'espresso divieto di eludere sistemi di controllo posti a presidio di, o al fine di restringere l'accesso a, sistemi informatici o telematici, e comunque di accedere ai predetti sistemi in mancanza delle necessarie autorizzazioni;

• l'espresso divieto di trasmettere o comunicare a terzi, o di acquisire a qualsiasi titolo da terzi, password, codici, dati o informazioni di sorta, atti a consentire al solo legittimo detentore l'accesso o la permanenza all'interno di sistemi informatici o telematici.

E.5. Procedure specifiche

Philogen attua tutti gli adempimenti previsti dalla legge, o comunque dettati dall'esperienza e dalle norme di buona tecnica, per garantire un adeguato e legittimo trattamento dei dati e conseguentemente la prevenzione dei reati informatici.

La società ha stabilito un Regolamento interno e delle procedure di sistema (Procedura n.° 1101-002 SICUREZZA DEI PERSONAL COMPUTER E DELLA RETE AZIENDALE, Procedure 1101-006 REVIEW OF ELECTRONIC AUDIT TRAIL, 1101-005 USER MANAGEMENT FOR CRITICAL SYSTEMS, 1101-004 COMPUTERIZED SYSTEM LIFE CYCLE) per l'utilizzo degli strumenti Informatici che viene pubblicizzato a tutti i livelli coinvolti come ordine di servizio (pubblicizzazione in bacheca, consegna copia a RSU, ecc.). Si tratta di disposizioni organizzative in materia di utilizzo della posta elettronica aziendale, di accesso e utilizzo di internet, di autenticazione informatica degli utenti, e più in generale di utilizzo del sistema informatico e trattamento dei dati (con particolare attenzione a dati ed informazioni riservati), di utilizzo di Notebook e telefoni cellulari.

È stato attribuito al responsabile dell'Area Informatica – nell'ambito delle rispettive competenze, ferme le necessarie esigenze di coordinamento – il compito di provvedere alle esigenze informatiche della Società, curando:

• la formulazione del relativo piano di investimenti, anche con il supporto di società/consulenti esterni;

• la definizione e corretta gestione dell'architettura dei sistemi informatici presenti all'interno della società (hardware, software e reti), ivi compresi i necessari presidi di controllo;

- le politiche di sicurezza e la predisposizione del piano di sviluppo informatico;
- la realizzazione e la cura della risorse informatiche.

In particolare, oltre agli adempimenti generali di cui al precedente paragrafo C.4:

- la Società ha provveduto alla formale nomina degli incaricati al trattamento dei dati personali, come da D.Lgs. 196/03 e s.m.i.;
- ha provveduto anche alla formale nomina degli amministratori di sistema interni ed esterni per la sicurezza dei dati e la prevenzione dei reati informatici, con relativa attribuzione ad essi dei necessari poteri e informativa specifica sui controlli cui il loro operato sarà sottoposto;
- la Società provvede alla costante verifica dell'effettivo recepimento e messa in pratica dei precetti posti dalle predette disposizioni organizzative, vigilando attraverso controlli periodici ed intervenendo tempestivamente al riguardo, in caso di eventuale inosservanza di regole e divieti.

La violazione delle disposizioni di cui alla presente Sezione della Parte Speciale, ed in genere delle disposizioni normative ed organizzative in tema di sicurezza informatica, espone alle sanzioni della Parte Generale.

DISCIPLINARE INTERNO PER IL PERSONALE DIPENDENTE

REGOLE ED OBBLIGHI IN RELAZIONE ALL'USO DEGLI STRUMENTI INFORMATICI, ALLA POSTA ELETTRONICA ED ALL'ACCESSO AD INTERNET

Revisione 31/07/2017

Disciplinare Interno contenente le Regole di condotta e gli obblighi dei dipendenti in relazione all'uso degli strumenti informatici, di internet e della posta elettronica

Sezione I

Art. 1 Premessa

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete Internet dai PC aziendali espone Philogen Spa (di seguito, Philogen o in generale, la Società) a possibili rischi di rilevanza sia civile, sia penale, sia amministrativa, creando potenziali problematiche alla sicurezza e all'immagine dell'Azienda stessa.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo da parte dei dipendenti delle risorse informatiche e telematiche dell'azienda, devono sempre ispirarsi al principio della diligenza e correttezza, Philogen ha adottato il presente Disciplinare Interno diretto ad evitare che condotte inconsapevoli possano innescare eventuali problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Il presente Disciplinare Interno si applica agli amministratori, ai dipendenti ed ai consulenti esterni che si trovino ad operare con gli strumenti informatici di Philogen.

Il presente Disciplinare Interno, è strutturato in sette sezioni nel modo che segue:

I Sezione (Premessa, Definizioni, Modalità d'uso generali dei PC)

II Sezione (Internet)

III Sezione (Posta Elettronica)

IV Sezione (PC, Palmare, altri dispositivi, Cellulare)

V Sezione (Applicazione e Controllo)

VI Sezione (Soggetti Preposti del Trattamento, Incaricati e Responsabili)

VII Sezione (Provvedimenti Disciplinari)

VIII Sezione (Esercizio dei diritti)

La presente sezione definisce le modalità di accesso e di uso corretto dei PC utilizzati dagli amministratori, dai dipendenti e dai consulenti esterni per lo svolgimento delle mansioni e degli incarichi assegnati.

Un uso dei PC e di altri dispositivi elettronici nonché dei servizi di internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare Interno potrebbe esporre Philogen alla minaccia di accessi non autorizzati al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico della Società e/o malfunzionamenti in generale dell'intero sistema informatico.

Articolo 2 Definizioni

TECNOLOGIA DELLA SOCIETA': comprende, in via esemplificativa e non esaustiva:

- l'hardware di elaborazione della Società (main frame, server, desktop, veicolari e laptop);
- il software (applicazioni che supportano i flussi di lavoro, i sistemi operativi, il software dei programmi di utilità);
- reti e applicazioni di rete (PDA, sistemi telefonici, audiomessaggeria, posta elettronica, fax);
- i server di collegamento alle borse per la ricerca dei dati di mercato e l'invio degli ordini.

PC: il sistema informatico consegnato al dipendente, incluse le periferiche, gli accessori ed il software. Di seguito anche "computer".

PALMARI - TABLET: il sistema informatico fornito al personale per eseguire operatività in modalità remota o smart working.

SOFTWARE: applicativo utilizzato dal PC che ne consenta il funzionamento e/o l'elaborazione delle informazioni o lo svolgimento di specifici compiti o funzioni, o che sia necessario per aumentare o diminuire la funzionalità di altri applicativi o del sistema operativo stesso.

FILE: qualunque tipo di documento elettronico, in qualsiasi formato, contenente dati, testo, immagini, suoni o un insieme degli stessi.

INTERNET: la rete informatica che consente, a livello mondiale, il collegamento e lo scambio di informazioni tra PC.

POSTA ELETTRONICA: software che consente l'invio di messaggi (e-mail) e documenti elettronici da un PC ad un altro utilizzando Internet.

LOGIN: Identificazione dell'utente (parte non segreta delle credenziali di autenticazione).

PASSWORD: il codice segreto individuale che permette l'autenticazione e l'accesso alla rete, a un PC, o più in generale a un sistema informatico protetto. È severamente vietato divulgare la password individuale a terzi (parte segreta delle credenziali di autenticazione).

DOWNLOAD: l'operazione che permette di trasferire un software o un file sul proprio PC prelevandolo dalla rete Internet o da altro PC o da un qualsiasi supporto magnetico, ottico o di qualunque altro tipo. UPLOAD: l'operazione che permette di trasferire un software o un file sulla rete Internet prelevandolo dal proprio computer o da altro computer o da un qualsiasi supporto magnetico, ottico o di qualunque altro tipo, collegato alla rete di Philogen.

LAN: la rete locale.

SERVER: il computer che utilizza software di gestione di altri computer, fornendo ad essi servizi su una rete, e gestione di file, stampanti, internet, dati.

CHAT: servizio di conversazione contemporanea tra utenti in tempo reale tramite lo scambio di messaggi di testo su rete locale o su internet.

BACKUP: copia di riserva di dati, di una serie di cartelle, di file effettuata su una memoria di massa o su qualsiasi altro supporto diverso dall'originale.

CRACKING PROGRAMS: software idonei a violare le protezioni o le password di altri software. INTERNET SERVICE PROVIDER: fornitore del servizio di accesso alla rete.

INFORMAZIONI RISERVATE: si intendono in via esemplificativa e non esaustiva:

- Informazioni relative all'attività di processo di produzione di molecole;
- le informazioni relative a pazienti sotto sperimentazione;
- le informazioni relative ai clienti o fornitori della società e in particolare ai servizi richiesti da essi alla società e/o ai documenti finanziari che li riguardino;
- le informazioni relative alle procedure, prodotti, organizzazione, gestione, progetti futuri, organizzazione del personale e documenti di proprietà della società;
- informazioni relative a tutti i lavoratori autonomi o subordinati o agli amministratori della società, comprese le informazioni riguardanti la loro retribuzione e il loro preavviso.

CED: dipartimento della società che si occupa della gestione, amministrazione e funzionamento delle infrastrutture informatiche. Al suo interno operano l'Amministratore di Sistema e i suoi preposti

Art. 3 Modalità d'uso del PC

Il sistema informativo aziendale è composto da un insieme di unità server centrali e macchine client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi.

Articolo 4 Casi di esclusione di utilizzo degli strumenti informatici

I casi di esclusione possono riguardare:

1. l'utilizzo del PC,
2. l'utilizzo della posta elettronica;
3. l'accesso a internet

Le eventuali esclusioni sono strettamente connesse alla natura delle mansioni. Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo coloro che per funzionalità societaria e lavorativa ne abbiano un effettivo e concreto bisogno.

Articolo 5 Corretto utilizzo del PC

Il PC consegnato ad amministratori, dipendenti e consulenti che utilizzino strumenti informatici di Philogen è uno strumento di lavoro e contiene tutti i software necessari a svolgere le mansioni affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da credenziali di autenticazione (login + password) che devono essere custodite dall'incaricato con la massima diligenza e non divulgate. La stessa password o diversa deve essere utilizzata anche per la funzionalità screen saver (= salva schermo). Le modalità per attivare lo screen saver se non conosciute possono essere richieste all'amministratore di sistema. Il PC che viene consegnato ad amministratori, dipendenti e consulenti contiene tutti i software necessari a svolgere le mansioni affidate. Per necessità aziendali, il dipartimento CED, utilizzando la propria login con privilegi di Amministratore e la password dell'Amministratore, potrà accedere, con le regole indicate nel presente documento, sia alla memoria di massa locale che al server aziendale nonché, previa comunicazione all'interessato, accedere al singolo PC in remoto.

In particolare chi utilizza un PC aziendale deve adottare le seguenti misure:

1) utilizzare solo ed esclusivamente le aree di memoria della Rete Philogen ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di Rete.

3. spegnere il PC ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio, e curarsi di effettuare il Logout, rendendo necessario un nuovo Login per poter effettuare altre operazioni (pressione simultanea tasti CTRL+ALT+CANC), poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

4. mantenere sul PC esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc), disposti dal CED.

Articolo 6 Espressi Divieti sull'utilizzo generale del PC

Ad amministratori, dipendenti e consulenti che utilizzino strumenti informatici di Philogen è vietato:

a) Registrare alcun file, software o archivio dati nel disco fisso o memoria di massa del PC consegnato al dipendente.

b) Modificare le configurazioni già impostate sul PC/ computer portatile / palmare consegnato.

c) Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta del diretto superiore gerarchico del dipendente e del CED.

d) Installare alcun software di cui la Philogen non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer (portatile o palmare) consegnato, senza l'espressa autorizzazione del CED. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.

e) Caricare sul disco fisso del PC consegnato al dipendente o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.

f) Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa del CED.

g) Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico della Philogen, quali per esempio virus, trojan horses ecc.

h) Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.

Sezione II - Internet

Articolo 6 Internet è uno strumento di lavoro

La connessione alla rete internet dal PC avuto in dotazione (sia portatili che palmari) è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione - nei limiti temporali delle pause autorizzate - e comunque con gli accorgimenti di cui al presente documento, senza oneri per la società e nel rispetto dei principi di decoro e di possibile inerenza con la mission aziendale.

Articolo 8 Misure preventive per ridurre navigazioni illegittime

Philogen ha adottato idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa (attraverso ad esempio filtri, Blacklist o Whitelist) di cui l'utente è a conoscenza mediante avviso immediatamente successivo alla installazione.

Articolo 9 Espressi Divieti concernenti Internet

È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.

È vietato all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'amministratore di sistema.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

È vietato al lavoratore di promuovere utile o guadagno personale attraverso l'uso di internet aziendale.

È vietato, infine, creare siti web personali sui sistemi della Philogen nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

Ogni eventuale navigazione di questo tipo (qualora non impedita dai filtri di cui all'articolo 7), comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è posta sotto la personale responsabilità dell'incaricato inadempiente.

Articolo 10 Divieti di Sabotaggio

È vietato al lavoratore di accedere ad alcuni siti internet mediante azione inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dalla Philogen per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

Articolo 11 Diritto d'autore

È vietato utilizzare l'accesso ad internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248).

Sezione III - Posta elettronica

Articolo 12 La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa: pertanto, l'uso per motivi personali è permesso con moderazione e comunque con gli accorgimenti di cui all'articolo seguente, senza oneri per la società e nel rispetto dei principi di decoro e di possibile inerenza con la mission aziendale.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Articolo 13 Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

Philogen consente un limitato utilizzo personale della posta elettronica da parte dei dipendenti come specificato sopra e allo scopo prevede le seguenti misure:

1) in caso di ricezione sulla email aziendale di posta personale la società raccomanda di cancellare ogni messaggio al fine di evitare un eventuale e possibile back up dei dati.

2) quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta, la società raccomanda di comunicare l'anomalia all'amministratore di sistema interno.

Articolo 14 Espressi Divieti nell'uso della posta elettronica

È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio della Philogen per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta della Philogen, nonché utilizzare il dominio della Philogen per scopi personali.

È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non collegati alo svolgimento della propria attività lavorativa.

È vietato spedire una e-mail con allegato un file eseguibile (.exe) senza la previa autorizzazione scritta del diretto superiore gerarchico o del CED.

È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni alla Philogen informazioni riservate o comunque documenti aziendali, senza previa autorizzazione degli amministratori o se non oggetto di natura contrattuale con il destinatario.

È vietato inviare o archiviare messaggi in forma criptata (al di fuori di esigenze interne di Philogen) senza l'espressa autorizzazione degli amministratori. In caso di documenti riservati è possibile l'inoltro in modalità criptata solo a soggetti interni a Philogen, mediante i programmi messi a disposizione dal CED e quando previsto.

È infine vietato utilizzare la posta elettronica aziendale in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore.

Articolo 15 Posta Elettronica in caso di Assenze Programmate e Non Programmate

Il dipendente ha l'obbligo di attivare il servizio di risposta automatica (Auto-reply), attraverso le modalità comunicatogli dall'amministratore di sistema sia in caso di assenza programmata che in caso di assenza non programmata. In tale ultimo caso, peraltro, qualora il dipendente non possa attivare il servizio ha l'obbligo di avvertire il CED affinché provveda ad attivarlo.

In alternativa il dipendente deve nominare un collega fiduciario che in caso di assenza dell'incaricato inoltri i files necessari all'attività lavorativa a chi ne abbia urgenza.

Articolo 16 Utilizzo Illecito di Posta Elettronica

È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, messaggi o materiale che possano ritenersi offensivi dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico/sindacale.

E' vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, o che possano in qualche modo essere discriminatori per razza, fede religiosa, età, genere, cittadinanza, stato civile, svantaggio fisico o psichico, ecc.

Qualora il dipendente riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'amministratore di sistema.

Sezione IV

Uso del PC portatile, del palmare, del cellulare e di altri dispositivi elettronici

Il PC portatile, il palmare, il cellulare e il veicolare - concessi in uso dalla Società agli amministratori, ai dipendenti e ai consulenti per specifici incarichi di spostamento, devono essere utilizzati secondo quanto specificato di seguito.

Articolo 17 Utilizzo del PC portatile, del palmare o di altri dispositivi elettronici

Gli amministratori, i dipendenti e i consulenti per specifici incarichi che ne prevedano l'utilizzo sono responsabili del PC portatile, del palmare, del veicolare e degli altri dispositivi elettronici assegnati loro dall'amministrazione di sistema e devono custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili e veicolari si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili, il palmare e gli altri dispositivi elettronici utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

In caso di perdita o furto dei PC portatili, del palmare e degli altri dispositivi elettronici deve far seguito la denuncia alle Autorità competenti. Allo scopo si deve avvisare immediatamente l'amministratore di sistema che provvederà – se del caso – ad occuparsi delle procedure connesse alla Privacy.

Agli amministratori, ai dipendenti e ai consulenti per specifici incarichi è vietato lasciare il PC portatile o il palmare in luoghi visibili, quando incustoditi (ad es. a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali, ecc.). Essi hanno l'obbligo di portare con sé il PC portatile o il palmare dopo l'orario di lavoro. Anche di giorno, durante l'orario di lavoro a nessuno è consentito lasciare incustodito il PC portatile o il palmare in zone e aree molto frequentate.

I collaboratori operanti sui mezzi semoventi hanno l'obbligo di mantenere in condizioni di pulizia ed efficienza il veicolare di bordo, segnalando con tempestività ogni anomalia o malfunzionamento.

Sezione V Applicazione e controllo

Articolo 18 Modalità di verifica

In applicazione del principio di necessità e di proporzionalità di cui dlgs 196/03 e GDPR 679/2016, Philogen promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici, come illustrato nel presente Disciplinare Interno.

Philogen informa di aver adottato dei sistemi che evitano qualunque interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. In particolare detti sistemi atti a monitorare in modalità anonima e aggregata eventuali violazioni di legge o comportamenti anomali da parte dei dipendenti avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche. Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) verrà avvisata l'area di riferimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. In caso di ulteriori comportamenti illeciti la Philogen tenterà di

individuare il colpevole attraverso verifiche graduali e potrà prevedere i provvedimenti disciplinari indicati alla successiva sezione VII, naturalmente con riferimento ai soli amministratori, lavoratori dipendenti e consulenti se incaricati per attività specifiche che prevedano l'uso di sistemi informativi di proprietà Philogen.

Articolo 19 Modalità di Conservazione

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Sezione VI

Soggetti Preposti del Trattamento, Incaricati e Responsabili

Articolo 20 Individuazione dei Soggetti autorizzati

Philogen ha designato formalmente gli incaricati al trattamento, cui ha impartito precise istruzioni sulle modalità di trattamento.

Per quanto riguarda i soggetti preposti alla manutenzione dei dati sono stati appositamente incaricati di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza realizzare attività di controllo a distanza, neanche di propria iniziativa.

I soggetti che operano quali amministratori di sistema o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sono consapevoli sugli aspetti legali e tecnico- gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sulla riservatezza nelle comunicazioni.

Sezione VII Provvedimenti disciplinari

Articolo 21 Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Disciplinare Interno potranno essere punite, a seconda della gravità delle mancanze, con i provvedimenti previsti dal Sistema Disciplinare riportato nella sezione 3 del Modello Organizzativo di Philogen, nel rispetto della vigente normativa e del contratto colletivo di lavoro applicato.

Articolo 22 Modalità di adozione delle Sanzioni verso i dipendenti

Le sanzioni disciplinari di cui all'art. 21 dovranno essere adottate nel rispetto della procedura di cui all'art. 7 della legge n. 300 del 20 maggio 1970 e dell'art. 157 del contratto collettivo nazionale per i lavoratori del terziario, distribuzione e servizi e per i dipendenti ed operatori di vendita.

L'azienda infatti non può adottare i provvedimenti disciplinari nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa.

Il lavoratore può farsi assistere da un rappresentante dell'organizzazione sindacale cui eventualmente aderisce o conferisce mandato.

In ogni caso i provvedimenti disciplinari più gravi del richiamo verbale non possono essere applicati prima che siano trascorsi 5 giorni dalla contestazione per iscritto del fatto che vi ha dato causa: nel corso di tale periodo il lavoratore potrà presentare le sue giustificazioni.

Se il provvedimento non verrà emanato entro 15 giorni dalla presentazione delle giustificazioni da parte del lavoratore, le giustificazioni stesse s'intenderanno accolte, a meno che durante tale periodo l'azienda non sia venuta in possesso di tutti gli elementi di giudizio e di tale circostanza abbia informato per iscritto, entro il predetto termine, il lavoratore.

Non si tiene conto ad alcun effetto delle sanzioni disciplinari, decorsi 2 anni dalla loro applicazione.

Articolo 23 Modalità di adozione delle Sanzioni verso gli amministratori e i consulenti

Le sanzioni disciplinari di cui all'art. 21 dovranno essere adottate nel rispetto del "Sistema Disciplinare" del Modello Organizzativo ex. D.Lgs. 231/01.

Sezione VIII

Esercizio dei diritti dell'interessato

Articolo 23 Modalità di Esercizio dei diritti

Il dipendente, interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere ai sensi dell'art. 7 alle informazioni che lo riguardano scrivendo a Philogen S.p.A. presso la sede sociale della stessa.