

**SEWS CABIND S.p.A.**  
**Modello di organizzazione, gestione e controllo ex D.Lgs. 231/2001**  
**Approvato dal Consiglio di Amministrazione in data 25/11/2009**

Indice

|  |           |
|--|-----------|
| <b>1. Il Decreto Legislativo n. 231/2001 e la normativa rilevante.</b>   | <b>4</b>  |
| <b>2 Il Modello di Organizzazione, Gestione e Controllo di SEWS-Cabind</b>                                     | <b>7</b>  |
| 2.1 La costruzione del Modello   | 7         |
| 2.2 La funzione del Modello  | 8         |
| 2.3 Il Modello nel contesto di SEWS-Cabind   | 9         |
| 2.4 Adozione del Modello e successive modifiche di adeguamento e aggiornamento dello stesso                    | 10        |
| <b>3. I Processi Sensibili di SEWS-Cabind</b>  | <b>11</b> |
| <b>4. Organismo di Vigilanza (o OdV)</b>   | <b>12</b> |
| 4.1. Premessa  | 12        |
| 4.2. Compiti, requisiti e poteri dell'Organismo di Vigilanza   | 12        |
| 4.3 Funzioni e poteri dell'Organismo di Vigilanza  | 17        |
| 4.4 Attività di relazione dell'Organismo di Vigilanza verso il vertice aziendale                               | 19        |
| 4.5 Flussi informativi verso l'OdV: informazioni di carattere generale ed informazioni specifiche obbligatorie | 20        |
| 4.6 Raccolta e conservazione delle informazioni  | 21        |
| 4.7 La formazione delle risorse e la diffusione del Modello  | 22        |
| <b>5 Sanzioni Disciplinari</b>   | <b>22</b> |
| 5.1 Premessa   | 22        |
| 5.2 Misure nei confronti di quadri, impiegati ed operai - Sistema disciplinare                                 | 24        |
| 5.3 Violazioni del Modello e relative sanzioni   | 24        |
| 5.4 Misure nei confronti dei dirigenti   | 26        |
| 5.5 Misure nei confronti degli Amministratori  | 26        |
| <b>6. Verifiche sull'adeguatezza del Modello</b>   | <b>26</b> |
| <b>SEZIONE I I reati nei rapporti con la P.A.</b>  | <b>28</b> |
| <b>1.Corruzione e concussione</b>  | <b>28</b> |
| <b>2.Truffa aggravata ai danni dello Stato</b>   | <b>30</b> |
| <b>3. Frode Informatica</b>  | <b>30</b> |
| <b>4. Reati in tema di erogazioni pubbliche</b>  | <b>31</b> |
| <b>5. Processi Sensibili nei rapporti con la P.A.</b>  | <b>32</b> |
| 5.1 Regole generali: l'organizzazione della Società  | 32        |
| 5.2 La struttura organizzativa   | 32        |
| 5.3 Le deleghe   | 32        |
| 5.4 Le procure   | 33        |

|  |           |
|--|-----------|
| <b>6. Regole generali: i principi generali di comportamento</b>  | <b>33</b> |
| 6.1 Nei rapporti con pubblici funzionari   | 33        |
| 6.2 Nell'offerta di omaggi   | 34        |
| 6.3 Nel rilascio di dichiarazioni alla P.A. e nella richiesta ed utilizzo di finanziamenti pubblici  | 34        |
| <b>7. Procedure specifiche</b>   | <b>35</b> |
| 7.1 Nella gestione delle Operazioni Sensibili  | 35        |
| 7.2 Nei rapporti con Consulenti e Partner  | 35        |
| 7.3 Nel rilascio di dichiarazioni alla P.A. e nella richiesta ed utilizzo di finanziamenti pubblici  | 35        |
| 7.4 Nelle ispezioni  | 36        |
| 7.5 Procedure già esistenti in SEWS-Cabind   | 36        |
| <b>8. Controlli dell'Organismo di Vigilanza</b>  | <b>36</b> |
| <b>SEZIONE II REATI SOCIETARI</b>  | <b>37</b> |
| <b>1. Reati Societari</b>  | <b>37</b> |
| <b>2. Funzioni della sezione II</b>  | <b>38</b> |
| <b>3. Processi Sensibili nell'ambito dei reati societari</b>   | <b>38</b> |
| <b>4. Regole generali</b>  | <b>38</b> |
| <b>5. Principi di comportamento e procedure specifiche</b>   | <b>39</b> |
| 5.1 Formazione del bilancio e predisposizione delle comunicazioni ai soci e/o ai terzi relative alla situazione economica, patrimoniale e finanziaria della Società                | 39        |
| 5.2 Operazioni relative al capitale sociale  | 40        |
| 5.3 Gestione dei rapporti con gli organi di controllo e formazione della volontà assembleare   | 41        |
| <b>6. False comunicazioni sociali – False comunicazioni sociali in danno della Società, dei soci e dei creditori</b>   | <b>41</b> |
| <b>7 Impedito Controllo - Art. 2625 del codice civile</b>  | <b>45</b> |
| <b>8. Illecita influenza sull'Assemblea - Art. 2636 del codice civile</b>  | <b>45</b> |
| <b>9. Aggiotaggio - Art. 2637 del codice civile</b>  | <b>45</b> |
| <b>10. Illecite operazioni sulle azioni o quote sociali o della società controllante - Art. 2628 del codice civile.</b>  | <b>46</b> |
| <b>11. Operazioni in pregiudizio dei creditori - Art. 2629 del codice civile.</b>  | <b>46</b> |
| <b>SEZIONE III REATI DI CRIMINALITÀ INFORMATICA</b>  | <b>48</b> |
| <b>SEZIONE IV RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO BENI O UTILITÀ DI PROVENIENZA ILLECITA</b>   | <b>59</b> |
| <b>SEZIONE V REATI CONTRO LA PERSONALITÀ INDIVIDUALE</b>   | <b>61</b> |
| <b>SEZIONE VI "REATI DI OMICIDIO COLPOSO E LESIONI PERSONALI COLPOSE GRAVI O GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO"</b> | <b>63</b> |

## DEFINIZIONI

- “**CCNL**”: Contratto Collettivo Nazionale di Lavoro per gli addetti all’industria metalmeccanica ed altri Contratti attualmente in vigore ed applicati da SEWS-Cabind;
- “**Consulenti**”: coloro che agiscono in nome e/o per conto di SEWS-Cabind sulla base di un mandato o di altro rapporto di collaborazione professionale;
- “**Dipendenti**”: tutti i dipendenti di SEWS-Cabind (compresi i dirigenti);
- “**D.Lgs. 231/2001**”: il decreto legislativo n. 231 dell’8 giugno 2001 e successive modifiche;
- “**Linee Guida**”: le Linee Guida per la costruzione dei modelli organizzazione, gestione e controllo *ex* D.Lgs. 231/2001 approvate da Confindustria in data 7 marzo 2002, aggiornate il 24 maggio 2004, e successive integrazioni;
- “**Modello**”: i modelli o il modello di organizzazione, gestione e controllo previsti dal D.Lgs. 231/2001;
- “**Organismo di Vigilanza**” o “**OdV**”: organismo interno preposto alla vigilanza sul funzionamento e sull’osservanza del Modello e al relativo aggiornamento;
- “**Operazione Sensibile**”: operazione o atto che si colloca nell’ambito dei Processi Sensibili di SEWS-Cabind;
- “**Organi Sociali**”: il Consiglio di Amministrazione e il Collegio Sindacale di SEWS-Cabind;
- “**P.A.**”: la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio;
- “**Partner**”: controparti contrattuali di SEWS-Cabind, quali ad es. società di servizi, agenti, partner, sia persone fisiche sia persone giuridiche, con cui la Società addivenga ad una qualunque forma di collaborazione contrattualmente regolata (società, associazione temporanea d’impresa, consorzi, ove destinati a cooperare con l’azienda nell’ambito dei Processi Sensibili);
- “**Processi Sensibili**”: attività di SEWS-Cabind nel cui ambito ricorre il rischio di commissione;
- “**Reati**”: i reati presupposto ai quali si applica la disciplina prevista dal D.Lgs. 231/2001;
- “**Società** o “**SEWS-Cabind**”: **SEWS-Cabind SPA**, con sede in Collegno, Torino, Corso Pastrengo, 40.

## SEZIONE GENERALE

### 1. IL DECRETO LEGISLATIVO N. 231/2001 E LA NORMATIVA RILEVANTE.

Il Decreto Legislativo 8 giugno 2001, n. 231, recante “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 amministrativa degli enti, che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito.

L’ampliamento della responsabilità mira a coinvolgere nella punizione di taluni illeciti penali il patrimonio degli enti e, in definitiva, gli interessi economici dei soci, i quali, fino all’entrata in vigore della legge in esame, non pativano conseguenze dalla realizzazione di reati commessi, con vantaggio della società, da amministratori e/o dipendenti. Il principio della personalità della responsabilità penale li lasciava, infatti, indenni da conseguenze sanzionatorie, diverse dall’eventuale risarcimento del danno, se ed in quanto esistente. Sul piano delle conseguenze penali, infatti, soltanto gli artt. 196 e 197 cod. pen. prevedevano (e prevedono tutt’ora) un’obbligazione civile per il pagamento di multe o ammende inflitte, ma solo in caso d’insolvibilità dell’autore materiale del fatto.

L’innovazione normativa, perciò, è di notevole rilevanza, 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.

Quanto alla tipologia di reati cui si applica la disciplina in esame, il legislatore delegato ha operato dapprima una scelta minimalista rispetto alle indicazioni contenute nella legge delega (l. n. 300/2000). Infatti, delle quattro categorie di reati indicate nella legge n. 300/2000, il Governo ha preso in considerazione soltanto quelle indicate 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 esteso il catalogo dei reati cui si applica la disciplina del decreto n. 231/2001.

La legge 23 novembre 2001, n. 4092, 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 (l’art. 25-bis) relativo alle falsità in monete, carte di pubblico credito e in valori di bollo.

L’intervento più importante è però rappresentato dal D. Lgs. n. 61/2002 in tema di reati societari, 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 la 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, 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, aggio, 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 ha inserito un nuovo art. 25-quater al decreto 231, che stabilisce la responsabilità amministrativa dell'ente anche in relazione 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" 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 (art. 9) che, tra l'altro, ha recepito mediante norme di immediata applicazione la direttiva 2003/6/CE del Parlamento europeo e del Consiglio, del 28 gennaio 2003, relativa all'abuso di 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.

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 di informazioni privilegiate (c.d. *insider trading*) e della manipolazione del mercato.

La Legge Comunitaria 2004, in particolare, è intervenuta sia sul codice civile che sul Testo Unico della Finanza (TUF). Quanto al codice civile, è stato modificato l'art. 2637, che sanzionava il reato di aggio commesso su strumenti finanziari sia quotati che non quotati. La norma si applica invece adesso ai soli casi di aggio 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 società emittenti disciplinate dal TUF la nuova fattispecie dell'*insider trading* (o abuso di 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 di 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, che vieta e punisce le c.d. pratiche di infibulazione, dalla legge n. 38/2006, 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 del 15 novembre 2000.

La legge sulla prevenzione e divieto delle c.d. pratiche di infibulazione ha esteso l'ambito di applicazione del D. Lgs. n. 231/2001 al nuovo reato di pratiche di mutilazione degli organi genitali femminili (art. 583-bis c.p.).

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").

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.

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 verificano in connessione alla violazione delle norme per la prevenzione degli infortuni sul lavoro o relative alla tutela dell'igiene e della salute sul lavoro.

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 criminose e di finanziamento del terrorismo (c.d. III Direttiva antiriciclaggio). 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.

La legge 18 marzo 2008, n. 48, di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, amplia ulteriormente la categoria dei nuovi reati presupposto per l'applicazione della responsabilità amministrativa degli enti, ai sensi del D. Lgs. 231/2001.

La legge n. 99 del 23 luglio 2009 ha introdotto nuovi reati presupposto: i reati in materia di proprietà industriale e violazione del diritto di autore e i delitti contro l'industria ed il commercio.

La legge n. 94 del 15 luglio 2009 ha ulteriormente ampliato le fattispecie connesse con la criminalità organizzata ed infine, la legge n. 116 del 3 agosto 2009 ha introdotto il reato di "induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria".

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 a 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 esercitano 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.

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 che la condotta illecita sia stata realizzata nell'interesse o a vantaggio di esso. Dunque, non soltanto allorché 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.

L'art. 6 del provvedimento in esame contempla tuttavia una forma di "esonero" da responsabilità dell'ente se si dimostra, in occasione di un procedimento penale per uno dei reati considerati, di aver adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione degli illeciti penali considerati. Il sistema prevede l'istituzione di un organo di controllo interno all'ente con il compito di vigilare sull'efficacia reale del modello. La norma stabilisce, infine, che le associazioni di categoria possono disegnare i codici di comportamento, sulla base dei quali andranno elaborati i singoli modelli organizzativi, da comunicare al Ministero della Giustizia, che ha trenta giorni di tempo per formulare le proprie osservazioni.

Il sistema di "esonero", indicato dalla legge, pone all'interprete numerosi interrogativi sia sull'inquadramento dogmatico degli istituti che operano nel suo ambito, sia sul rilievo pratico che essi possono avere. Non è facile, ad esempio, definire la funzione ed il ruolo della comunicazione al Ministero della Giustizia dei codici di comportamento redatti dalle associazioni di categoria.

Evitando di occuparci della natura giuridica e dell'inquadramento dogmatico delle soluzioni accolte dal legislatore, qui giova soffermare l'attenzione sugli aspetti pratici, che possono interessare gli operatori coinvolti dal provvedimento di legge. Va sottolineato, in proposito, che l'"esonero" dalle responsabilità dell'ente passa attraverso il giudizio d'idoneità del sistema interno di organizzazione e controlli, che il giudice penale è chiamato a formulare in occasione del procedimento penale a carico dell'autore materiale del fatto illecito. Dunque, la formulazione dei modelli e l'organizzazione dell'attività dell'organo di controllo devono porsi come obiettivo l'esito positivo di tale giudizio d'idoneità. Questa particolare prospettiva finalistica impone agli enti di valutare l'adeguatezza delle proprie procedure alle esigenze di cui si è detto, tenendo presente che la disciplina in esame è già entrata in vigore.

È opportuno precisare che la legge prevede l'adozione del modello di organizzazione, gestione e controllo in termini di facoltatività e non di obbligatorietà. La mancata adozione non è soggetta, perciò, ad alcuna sanzione, ma espone l'ente alla responsabilità per gli illeciti realizzati da amministratori e dipendenti. Pertanto, nonostante la ricordata facoltatività del comportamento, di fatto, l'adozione del modello diviene obbligatoria se si vuole beneficiare dell'esimente.

Pertanto la SEWS-Cabind S.p.A. ha deciso di redigere e di adottare il seguente modello organizzativo.

## **2 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI SEWS-CABIND**

### **2.1 La costruzione del Modello**

Successivamente all'emanazione del D.Lgs. 231/2001, SEWS-Cabind ha avviato un progetto interno finalizzato a garantire la predisposizione del Modello di cui all'art. 6 del citato Decreto.

La predisposizione del presente Modello è stata preceduta da una serie di attività preparatorie suddivise in differenti fasi e dirette tutte alla costruzione di un sistema di prevenzione e gestione dei rischi, in linea con le disposizioni del D.Lgs. 231/2001 e tenuto conto delle Linee Guida di Confindustria.

La Società ha conferito a propri professionisti (studio Jones Day, avv. Marini) l'effettuazione dell'analisi dei rischi che sono riassunti nel Memorandum "*Audit Report on compliance of SEWS-Cabind S.p.A. with the Provisions of Legislative Decree No. 231/2001*".

Si descrivono brevemente qui di seguito le fasi in cui si è articolato il lavoro di individuazione delle aree a rischio, sulle cui basi si è poi dato luogo alla predisposizione del presente Modello.

1) L'individuazione dei Processi Sensibili è stata attuata attraverso il previo esame della documentazione aziendale (principali procedure in essere, deleghe, procure, circolari interne, ecc.) e una serie di interviste con i soggetti chiave della struttura aziendale (Amministratore Delegato, Responsabile Amministrazione, Finanza e Contabilità, Direttore Qualità, Ambiente e Sicurezza, Direttore del Personale, Direttore Commerciale, Responsabile Ufficio Acquisti, Responsabile Progettazione e Produzione, Responsabile Information Technology) e all'interno delle singole direzioni, interviste mirate all'approfondimento dei Processi Sensibili e del controllo sugli stessi. Sono state altresì esaminate le procedure aziendali già adottate e attuate da SEWS-CABIND.

I risultati dell'attività sopra descritta sono stati valutati in sede di "Analisi del rischio" ove sono stati identificati i Processi Sensibili della Società nonché, nell'ambito dei medesimi, la descrizione dei controlli aziendali esistenti e le criticità rilevate. I Processi Sensibili di SEWS-CABIND sono quelli descritti al successivo cap. 3.

2) Effettuazione della "Analisi del rischio". Sulla base della rappresentazione della Società quale emergente dalla fase di identificazione dei Processi Sensibili (nonché descrizione dei controlli aziendali esistenti e relativa criticità) e in considerazione delle previsioni e delle finalità indicate dal D. Lgs. 231/2001, si è proceduto alla individuazione, nell'ambito dei Processi Sensibili, delle azioni di miglioramento delle attuali procedure interne e dei requisiti organizzativi essenziali per la definizione di un modello "specifico" di organizzazione, gestione e monitoraggio ai sensi del D. Lgs. 231/2001.

Ulteriore obiettivo di questa fase è stata l'individuazione, nell'ambito della struttura organizzativa della Società, delle aree aziendali ove è ravvisabile il rischio di commissione dei Reati.

3) **Predisposizione del Modello.** Il presente Modello è costituito da una "Sezione Generale", contenente i principi e le regole di carattere generale aventi rilevanza in merito alle tematiche disciplinate dal D.Lgs. 231/2001, e da singole "Parti Speciali" ciascuna delle quali predisposta per le diverse categorie di reato contemplate nel D.Lgs. 231/2001 astrattamente ipotizzabili nella Società in ragione dell'attività da questa svolta.

## **2.2 La funzione del Modello**

L'adozione e l'efficace attuazione del Modello non solo potrebbe consentire a SEWS-Cabind di beneficiare dell'esimente prevista dal D.Lgs. 231/2001, ma migliora, nei limiti previsti dallo stesso, il suo sistema di controllo interno limitando il rischio di commissione dei Reati.

Scopo del Modello è la predisposizione di un sistema strutturato ed organico di procedure ed attività di controllo preventivo che ha come obiettivo impedire la commissione dei Reati mediante la individuazione dei Processi Sensibili e la loro conseguente proceduralizzazione.

I principi contenuti nel presente Modello devono condurre, da un lato, a determinare una piena consapevolezza del potenziale autore del Reato di commettere un illecito (la cui commissione è fortemente condannata e contraria agli interessi di SEWS-Cabind, anche quando apparentemente essa potrebbe trarne un vantaggio), dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire a SEWS-Cabind di reagire tempestivamente nel prevenire od impedire la commissione del Reato stesso.

Tra le finalità del Modello vi è, quindi, quella di sviluppare la consapevolezza nei Dipendenti e Organi Sociali, che operino per conto o nell'interesse della Società nell'ambito dei Processi Sensibili di poter incorrere - in caso di comportamenti non conformi alle prescrizioni del Modello e alle altre procedure aziendali (oltre che alla legge) - in illeciti passibili di conseguenze penalmente rilevanti non solo per se stessi, ma anche per la Società.

Inoltre, si intende censurare fattivamente ogni comportamento illecito attraverso la costante attività dell'Organismo di Vigilanza sull'operato delle persone rispetto ai Processi Sensibili e la comminazione di sanzioni disciplinari o contrattuali.

### **2.3 Il Modello nel contesto di SEWS-Cabind**

Nella predisposizione del presente Modello si è tenuto conto delle procedure e dei sistemi di controllo esistenti e già ampiamente operanti in azienda, ove giudicati idonei a valere anche come misure di prevenzione dei Reati e strumenti di controllo sui Processi Sensibili.

Conformemente a quanto previsto anche dalle Linee Guida, sono stati considerati quali generali elementi costitutivi del Modello il sistema di controllo interno, il sistema di controllo della gestione e le *policy* e le procedure che lo compongono e, in particolare:

- il Codice Etico ed il Manuale del Dipendente;
- la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale e organizzativa;
- la comunicazione al personale e la formazione dello stesso;
- il sistema amministrativo, contabile e finanziario;
- il sistema disciplinare di cui al CCNL;
- il Sistema di Gestione della Qualità;
- il Sistema di Gestione di Ambiente;
- il sistema di certificazione OHSAS (*Occupational Health and Safety Assessment Series*) 18001;
- procedure all'interno dei controlli J-SOX;
- le direttive generali e politiche in materia di infrastrutture informatiche.

**Il presente Modello, fermo restando la sua finalità peculiare relativa al D.Lgs. 231/2001, si inserisce quindi nel più ampio sistema di controllo costituito principalmente dal sistema normativo interno già in essere in SEWS-Cabind.**

Principi cardine a cui il Modello si ispira sono: i requisiti indicati dal D.Lgs. 231/2001 ed in particolare:

- l'attribuzione ad un **Organismo di Vigilanza (OdV)** interno a SEWS-Cabind del compito di promuovere l'attuazione efficace e corretta del Modello anche attraverso il monitoraggio dei comportamenti aziendali ed il diritto ad una informazione costante sulle attività rilevanti ai fini del D.Lgs. 231/2001; la messa a disposizione dell'OdV di **risorse** adeguate a supportarlo nei compiti affidatigli ed a raggiungere i risultati ragionevolmente ottenibili;
- l'attività di **verifica del funzionamento** del Modello con conseguente aggiornamento periodico;
- l'attività di **sensibilizzazione e diffusione** a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- i principi generali di un adeguato sistema di controllo interno ed in particolare: la **verificabilità e documentabilità** di ogni operazione rilevante ai fini del D.Lgs. 231/2001; il rispetto del principio della **separazione delle funzioni**; la definizione di **poteri autorizzativi coerenti** con le responsabilità assegnate; la **comunicazione all'OdV delle informazioni rilevanti**.

## **2.4 Adozione del Modello e successive modifiche di adeguamento e aggiornamento dello stesso**

SEWS-Cabind ha adottato il proprio Modello con la delibera del Consiglio di Amministrazione del xxxxx e con la medesima delibera ha istituito il proprio Organismo di Vigilanza.

Nella predetta riunione, ciascun membro del Consiglio di Amministrazione ha espressamente dichiarato di impegnarsi al rispetto del presente Modello. Analogamente ciascun membro del Collegio Sindacale, presa visione del Modello, si è espressamente impegnato al rispetto del Modello medesimo.

Essendo il presente Modello un “atto di emanazione dell’organo dirigente” (in conformità alle prescrizioni dell’art. 6, comma 1, lettera *a*) del D.Lgs. 231/2001) le successive modifiche e integrazioni sono rimesse alla competenza del Consiglio di Amministrazione di SEWS-Cabind.

L’Organismo di Vigilanza, titolare di precisi compiti e poteri in merito alla cura, sviluppo e promozione del costante aggiornamento del Modello, individua e cura la redazione delle modifiche e/o integrazioni del Modello che si dovessero rendere necessarie in conseguenza di:

- violazioni delle prescrizioni del Modello;
- modificazioni dell’assetto interno organizzativo della Società e/o delle modalità di svolgimento delle proprie attività;
- modifiche normative;
- risultanze dei controlli;

e le sottopone per la relativa discussione ed approvazione al Consiglio di Amministrazione .

Il Consiglio di Amministrazione delibera quindi in merito all’aggiornamento e adeguamento del Modello sulla base delle modifiche e/o integrazioni allo stesso sottoposte.

Una volta approvate le modifiche, l’Organismo di Vigilanza provvede, senza indugio, a rendere le stesse operative e a curare la corretta comunicazione dei contenuti all’interno e all’esterno della Società.

Al fine di garantire che le variazioni del Modello siano operate con la necessaria tempestività ed efficacia, senza al contempo incorrere in difetti di coordinamento tra i processi operativi, le prescrizioni contenute nel Modello e la diffusione delle stesse, il Consiglio di Amministrazione ha altresì la facoltà di delegare al Presidente o all’Amministratore Delegato il compito di aggiornare il Modello.

Il Consiglio di Amministrazione ratifica quindi annualmente tutte le modifiche eventualmente apportate dal Presidente o dall’Amministratore Delegato. In pendenza di ratifica da parte del Consiglio di Amministrazione, le modifiche apportate dal Presidente o dall’Amministratore Delegato devono considerarsi pienamente valide e produttive di effetti.

### 3. I PROCESSI SENSIBILI DI SEWS-CABIND

SEWS-Cabind ha come oggetto sociale:

la produzione, l'assemblaggio, la commercializzazione e la progettazione di cablaggi, cavi ed impianti elettrici per l'industria, con particolare riferimento al settore dei veicoli.

Per il raggiungimento dello scopo sociale la Società potrà compiere operazioni mobiliari, immobiliari e finanziarie di qualsiasi specie (esclusa la raccolta del risparmio e l'esercizio del credito), compreso il rilascio di garanzie reali e personali a favore proprio o di terzi.

La Società potrà assumere partecipazioni e cointeressenze in altre società od enti, consorzi ecc., aventi scopo analogo, affine o complementare al proprio, al fine di stabile investimento e non collocamento.

Le operazioni di carattere finanziario non potranno essere svolte nei confronti del pubblico.

Il capitale sociale è di Euro 30.000.000,00 (trenta milioni).

#### Proprietà:

Sumitomo Electric Industries Limited (Giappone) Euro 16.200.000,00 (54%)

Sumitomo Wiring Systems Limited (Giappone) Euro 10.800.000,00 (36%)

Sumitomo Electric Wiring (Europe) Systems Limited (Gran Bretagna) Euro 3.000.000,00 (10%)

La Società è soggetta alla direzione ed al coordinamento di Sumitomo Electric Industries Limited.

SEWS-Cabind spa ha società controllate in Polonia (*SEWS-Cabind Poland Sp.zo.o.*) e Marocco (*SEWS-Cabind Maroc SA*) ed approva ogni anno il bilancio consolidato ai sensi della legge applicabile.

Il Consiglio di Amministrazione in carica è composto da 6 membri: Inoue Osamu (Presidente); Iba Junichi (Amministratore Delegato); Sotome Hiroshi (Amministratore Delegato); Saka Masamori (Consigliere); Lawson Michael James (Consigliere) e Masato Iguchi (Consigliere);

Procuratori: Massimo Magno; Riccardo Primon; Gianluca Durando.

Il Collegio Sindacale è composto da 3 membri effettivi e 2 supplenti.

La società di revisione è KPMG S.p.A.

Dall'analisi dei rischi condotta nell'ambito dell'attività aziendale di SEWS-Cabind ai fini del D.Lgs. 231/2001, è emerso che i Processi Sensibili della Società riguardano allo stato principalmente:

- i reati in materia di sicurezza sul lavoro;
- le relazioni con la P.A.;
- i reati societari.

Esistono invece rischi bassi di commissione dei seguenti reati:

- reati contro la personalità individuale;

- reati in materia di ricettazione e riciclaggio;
- reati informatici.

Gli altri reati contemplati dal D.Lgs. 231/2001 non appaiono concretamente configurabili nella realtà di SEWS-Cabind.

Le attività che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei reati di cui al D.Lgs. 231/2001, sono elencate in dettaglio nelle rispettive Parti Speciali. Seguendo l'evoluzione legislativa o quella dell'attività aziendale, l'OdV ha il potere di individuare eventuali ulteriori attività a rischio che potranno essere inserite nell'elenco dei Processi Sensibili.

## **4. ORGANISMO DI VIGILANZA (O ODV)**

### **4.1. Premessa**

L'art. 6 del D. Lgs. n. 231/2001 prevede che l'ente possa essere esonerato dalla responsabilità conseguente alla commissione dei reati indicati se l'organo dirigente ha, fra l'altro:

- a) adottato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
- b) affidato il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo (di seguito l'Organismo).

L'affidamento di detti compiti all'Organismo ed, ovviamente, il corretto ed efficace svolgimento degli stessi sono, dunque, presupposti indispensabili per l'esonero dalla responsabilità, sia che il reato sia stato commesso dai soggetti "apicali" (espressamente contemplati dall'art.6), che dai soggetti sottoposti all'altrui direzione (di cui all'art. 7).

L'art. 7, co. 4, ribadisce, infine, che l'efficace attuazione del Modello richiede, oltre all'istituzione di un sistema disciplinare, una sua verifica periodica, evidentemente da parte dell'organismo a ciò deputato.

Da quanto sopra sinteticamente richiamato, si rileva l'importanza del ruolo dell'Organismo, nonché la complessità e l'onerosità dei compiti che esso deve svolgere.

Per una corretta configurazione dell'Organismo è necessario valutare attentamente i compiti ad esso espressamente conferiti dalla legge, nonché i requisiti che esso deve avere per poter svolgere in maniera adeguata i propri compiti.

### **4.2. Compiti, requisiti e poteri dell'Organismo di Vigilanza**

Le attività che l'Organismo è chiamato ad assolvere, anche sulla base delle indicazioni contenute negli artt. 6 e 7 del D. Lgs. n. 231/2001, possono così schematizzarsi:

- vigilanza sull'effettività del modello, che si sostanzia nella verifica della coerenza tra i comportamenti concreti ed il modello istituito;
- disamina in merito all'adeguatezza del modello, ossia della sua reale (e non meramente formale) capacità di prevenire, in linea di massima, i comportamenti non voluti;
- analisi circa il mantenimento nel tempo dei requisiti di solidità e funzionalità del modello;

- cura del necessario aggiornamento in senso dinamico del modello, nell'ipotesi in cui le analisi operate rendano necessario effettuare correzioni ed adeguamenti. Tale cura, di norma, si realizza in due momenti distinti ed integrati:
- presentazione di proposte di adeguamento del modello verso gli organi/funzioni aziendali in grado di dare loro concreta attuazione nel tessuto aziendale. A seconda della tipologia e della portata degli interventi, le proposte saranno dirette verso le funzioni di Direzione Risorse Umane, Amministrazione, ecc., o, in taluni casi di particolare rilevanza, verso il Consiglio di Amministrazione;
- *follow-up*, ossia verifica dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte.

Si tratta di attività specialistiche, prevalentemente di controllo, che presuppongono la conoscenza di tecniche e strumenti *ad hoc*, nonché una continuità di azione elevata.

L'estensione dell'applicazione del decreto 231 ai delitti colposi pone un problema di rapporti tra il piano della sicurezza e quello del modello organizzativo, nonché tra le attività dei soggetti responsabili dei controlli in materia di salute e sicurezza sul lavoro e l'organismo di vigilanza. L'autonomia di funzioni proprie di questi organi non consente di ravvisare una sovrapposizione dei compiti di controllo, che sarebbe quindi tanto inutile quanto inefficace.

Deve essere chiaro pertanto, che i diversi soggetti deputati al controllo svolgono i propri compiti su piani differenti.

Questi elementi, sommati all'indicazione contenuta nella Relazione di accompagnamento al D. Lgs. n. 231/2001 che, in merito all'Organismo, parla di "(...) una struttura che deve essere costituita al suo (dell'ente) interno (...)", inducono ad escludere il riferimento al Consiglio di Amministrazione.

Fatta questa esclusione, è però opportuno precisare sin da ora che il massimo vertice societario (es. Consiglio di Amministrazione o Amministratore Delegato), pur con l'istituzione dell'Organismo ex D. Lgs. n. 231/2001, mantiene invariate tutte le attribuzioni e le responsabilità previste dal Codice Civile, alle quali si aggiunge oggi quella relativa all'adozione ed all'efficacia del Modello, nonché all'istituzione dell'Organismo [art. 6, co. 1, lett. a) e b)].

Considerazioni in parte analoghe possono svolgersi per il Collegio sindacale. Sotto il profilo della professionalità quest'organo sembra ben attrezzato per adempiere efficacemente al ruolo di vigilanza sul Modello. Per contro, appare più arduo riscontrare la necessaria continuità di azione che il legislatore ha inteso attribuire all'Organismo.

Va, inoltre, tenuto presente che l'attività di esso può essere oggetto di controllo (in particolare con riferimento al delitto di false comunicazioni sociali) ai sensi del D. Lgs. n. 231/2001.

È evidente, peraltro, che il Collegio sindacale, per la notevole affinità professionale e per i compiti che gli sono attribuiti dalla Legge, sarà uno degli interlocutori "istituzionali" dell'Organismo.

I sindaci, infatti, essendo investiti della responsabilità di valutare l'adeguatezza dei sistemi di controllo interno, dovranno essere sempre informati dell'eventuale commissione dei reati considerati, così come di eventuali carenze del Modello.

In taluni casi, rientranti nella patologia aziendale, poi, l'Organismo potrà riferire al Collegio sindacale affinché questo si attivi secondo quanto previsto dalla legge.

Occorre ora verificare se, nell'ambito delle varie forme che assume in concreto il disegno organizzativo

aziendale, esiste già - negli enti destinatari della norma ed, in particolare, nelle società di medio-grandi dimensioni - una struttura che possiede i requisiti necessari per assolvere il mandato ed essere, quindi, identificata nell'Organismo voluto dal D. Lgs. n. 231/2001.

A questo scopo appare opportuno riassumere sinteticamente quelli che appaiono i principali requisiti dell'Organismo.

- Autonomia ed indipendenza

L'interpretazione di questi requisiti ha determinato non pochi dubbi e perplessità. È chiaro che, ad esempio, il pagamento di un compenso alla persona, interna o esterna all'ente, per l'attività in argomento non costituisce causa di "dipendenza".

I requisiti vanno intesi in relazione alla funzionalità dell'Odv e, in particolare, ai compiti che la legge assegna allo stesso (sui requisiti dei singoli componenti si dirà tra breve). La posizione dell'Odv nell'ambito dell'ente deve garantire l'autonomia dell'iniziativa di controllo da ogni forma d'interferenza e/o di condizionamento da parte di qualunque componente dell'ente (e in particolare dell'organo dirigente). Tali requisiti sembrano assicurati dall'inserimento dell'Organismo in esame come unità di staff in una posizione gerarchica la più elevata possibile e prevedendo il "riporto" al massimo Vertice operativo aziendale ovvero al Consiglio di Amministrazione nel suo complesso.

Per assicurare la necessaria autonomia di iniziativa e l'indipendenza è poi indispensabile che all'Odv non siano attribuiti compiti operativi che, rendendolo partecipe di decisioni ed attività operative, ne minerebbero l'obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello.

Con riferimento all'Odv a composizione plurisoggettiva ci si deve chiedere se i requisiti di autonomia ed indipendenza siano riferibili all'Organismo in quanto tale ovvero ai suoi componenti singolarmente considerati. Si ritiene che con riferimento ai componenti dell'Organismo reclutati all'esterno i requisiti di autonomia ed indipendenza debbano essere riferiti ai singoli componenti. Al contrario, nel caso di composizione mista dell'Organismo, non essendo esigibile dai componenti di provenienza interna una totale indipendenza dall'ente, il grado di indipendenza dell'Organismo dovrà essere valutato nella sua globalità.

Anche in questo caso, tuttavia, conformemente alle prime indicazioni giurisprudenziali, i componenti interni dell'Odv non dovrebbero svolgere, nell'ambito dell'ente o di soggetti da questo controllati o che lo controllano, funzioni operative.

- Professionalità

Questo connotato si riferisce al bagaglio di strumenti e tecniche che l'Organismo deve possedere per poter svolgere efficacemente l'attività assegnata. Si tratta di tecniche specialistiche proprie di chi svolge attività "ispettiva", ma anche consulenziale di analisi dei sistemi di controllo e di tipo giuridico e, più in particolare, penalistico.

Con riferimento, invece, alle competenze giuridiche, non va dimenticato che la disciplina in argomento è in buona sostanza una disciplina penale e che l'attività dell'Odv (ma forse sarebbe più corretto dire dell'intero sistema di controllo previsto dal decreto in parola) ha lo scopo di prevenire la realizzazione di reati.

È dunque essenziale la conoscenza della struttura e delle modalità realizzative dei reati, che potrà essere assicurata mediante l'utilizzo delle risorse aziendali ovvero della consulenza esterna.

A questo riguardo, per quanto concerne le tematiche di tutela della salute e sicurezza sul lavoro, l'Odv dovrà avvalersi di tutte le risorse attivate per la gestione dei relativi aspetti (come detto, RSPP - Responsabile del Servizio di Prevenzione e Protezione, ASPP – Addetti al Servizio di Prevenzione e Protezione, RLS – Rappresentante dei Lavoratori per la Sicurezza, MC - Medico Competente, addetti primo soccorso, addetto emergenze in caso d'incendio), comprese quelle previste dalle normative di settore.

- Continuità di azione

Per poter dare la garanzia di efficace e costante attuazione di un modello così articolato e complesso, si rende necessaria la presenza di una struttura dedicata esclusivamente all'attività di vigilanza sul Modello priva, come detto, di mansioni operative che possano portarla ad assumere decisioni con effetti economico-finanziari.

Ciò non esclude, peraltro, che questa struttura possa fornire, come già detto, anche pareri consultivi sull'aggiornamento del Modello, pareri consultivi, infatti, non intaccano l'indipendenza e l'obiettività di giudizio su specifici eventi. Allo scopo di assicurare l'effettiva sussistenza dei descritti requisiti, sarà opportuno che i membri possiedano, oltre alle competenze professionali descritte, i requisiti soggettivi formali che garantiscano ulteriormente l'autonomia e l'indipendenza richiesta dal compito (es. onorabilità, assenza di conflitti di interessi e di relazioni di parentela con gli organi sociali e con il vertice, ecc.).

Al momento della formale adozione del Modello l'organo dirigente dovrà:

- disciplinare gli aspetti principali relativi al funzionamento dell'Organismo (es. modalità di nomina e revoca, durata in carica) ed ai requisiti soggettivi dei suoi componenti;

- comunicare alla struttura i compiti dell'Organismo ed i suoi poteri, prevedendo, in via eventuale, sanzioni in caso di mancata collaborazione.

In particolare, l'Organismo deve essere dotato di tutti i poteri necessari per assicurare una puntuale ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello organizzativo adottato dalla Società, secondo quanto stabilito dall'art. 6 del D. Lgs. n. 231/2001, e segnatamente per l'espletamento dei seguenti compiti:

a) verifica dell'efficienza ed efficacia del Modello organizzativo adottato rispetto alla prevenzione ed all'impedimento della commissione dei reati previsti dal D. Lgs. n. 231/2001;

b) verifica del rispetto delle modalità e delle procedure previste dal Modello organizzativo e rilevazione degli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni;

c) formulazione delle proposte all'organo dirigente per gli eventuali aggiornamenti ed adeguamenti del Modello organizzativo adottato, da realizzarsi mediante le modifiche e/o le integrazioni che si dovessero rendere necessarie in conseguenza di:

- \* significative violazioni delle prescrizioni del Modello organizzativo;

- \* significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa;

- \* modifiche normative;

d) segnalazione all'organo dirigente, per gli opportuni provvedimenti, di quelle violazioni accertate del Modello organizzativo che possano comportare l'insorgere di una responsabilità in capo all'ente.

e) predisposizione di una relazione informativa, su base almeno semestrale, per l'organo dirigente;

f) trasmissione della relazione di cui al punto precedente al Collegio sindacale.

Si precisa che:

- le attività poste in essere dall'Organismo non possono essere sindacate da alcun altro organismo o struttura aziendale, fermo restando però che l'organo dirigente è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo intervento, in quanto all'organo dirigente appunto rimonta la responsabilità ultima del funzionamento (e dell'efficacia) del modello organizzativo;

- l'Organismo ha libero accesso presso tutte le funzioni della Società - senza necessità di alcun consenso preventivo - onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal D. Lgs. n. 231/2001;

- l'Organismo può avvalersi - sotto la sua diretta sorveglianza e responsabilità - dell'ausilio di tutte le strutture della Società ovvero di consulenti esterni.

La definizione degli aspetti attinenti alla continuità dell'azione dell'Organismo, quali la calendarizzazione dell'attività, la verbalizzazione delle riunioni e la disciplina dei flussi informativi dalle strutture aziendali all'Organismo, potrà essere rimessa allo stesso Organismo, il quale in questi casi dovrà disciplinare il proprio funzionamento interno.

A tale proposito è opportuno che l'Organismo formuli un regolamento delle proprie attività (determinazione delle scadenze temporali dei controlli, individuazione dei criteri e delle procedure di analisi, ecc.). Non è, invece, opportuno che tale regolamento sia redatto ed approvato da organi societari diversi dall'Organismo di cui ci occupiamo giacché questo potrebbe far ritenere violata l'indipendenza dello stesso.

Alla luce di quanto sopra esposto SEWS-Cabind affiderà i compiti di OdV ad un organo collegiale, composto di tre persone provviste dei requisiti sopra descritti che sono state individuate dal Consiglio d'Amministrazione, previa valutazione dei Processi Sensibili di SEWS-Cabind.

E' pertanto rimesso a tale OdV il compito di svolgere le funzioni di vigilanza e controllo previste dal presente Modello.

L'OdV è inoltre individuato in condizione da assicurare un elevato affidamento quanto alla sussistenza dei requisiti soggettivi di eleggibilità che garantiscano ulteriormente l'autonomia e l'indipendenza richiesta dai compiti affidati.

In particolare, all'atto del conferimento dell'incarico, il CdA riceve, da parte del nominando OdV, la dichiarazione che attesta l'assenza di motivi di ineleggibilità quali, a titolo esemplificativo, l'onorabilità, l'assenza di conflitti di interessi e di relazioni di parentela con gli organi sociali e con il vertice.

Il conferimento dell'incarico di OdV e la revoca del medesimo (ad es. in caso violazione dei propri doveri derivanti dal presente Modello) sono atti riservati alla competenza del Consiglio di Amministrazione. L'incarico dell'OdV avrà una durata pari a tre anni, rinnovabili a ciascuna scadenza.

La revoca di tale incarico sarà ammessa soltanto per giusta causa.

A tale proposito, per "giusta causa" di revoca dei poteri connessi con l'incarico di membro dell'Organismo di Vigilanza potranno intendersi, a titolo meramente esemplificativo:

- motivi connessi al grave inadempimento – sia esso doloso o colposo – agli obblighi di cui all'incarico (esempio, infedeltà, inefficienza, negligenza, ecc.);

- l'“omessa o insufficiente vigilanza” da parte dell'OdV – secondo quanto previsto dall'art. 6, comma 1 lett. d), D.Lgs. 231/2001 – risultante da una sentenza di condanna, anche non passata in giudicato, emessa nei confronti della SEWS-Cabind ai sensi del D.Lgs. 231/2001 ovvero da sentenza di applicazione della pena su richiesta;
- casi di impossibilità sopravvenuta;
- il venir meno in capo all'OdV i requisiti di “autonomia e indipendenza” nonché di “continuità di azione”;
- qualora il membro dell'OdV sia un dipendente o un amministratore alla cessazione del rapporto di dipendenza o di amministrazione;
- morte del membro o sue dimissioni dall'incarico.

#### **4.3 Funzioni e poteri dell'Organismo di Vigilanza**

All'OdV è affidato il compito di vigilare:

- sull'osservanza del Modello da parte dei Dipendenti e degli Organi Sociali;
- sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati;
- sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative.

A tal fine, all'OdV sono altresì affidati i compiti di:

- proporre aggiornamenti;
- proporre agli organi o funzioni societarie competenti di emanare disposizioni procedurali di attuazione dei principi e delle regole contenute nel Modello;
- interpretare la normativa rilevante con l'eventuale assistenza di consulenti legali e verificare l'adeguatezza del Modello a tali prescrizioni normative, segnalando al Consiglio di Amministrazione le possibili aree di intervento;
- valutare le esigenze di aggiornamento del Modello, segnalando al Consiglio di Amministrazione le possibili aree di intervento;
- indicare alla dirigenza le opportune integrazioni ai sistemi di gestione delle risorse finanziarie (sia in entrata che in uscita), già presenti in SEWS-Cabind, per introdurre alcuni accorgimenti idonei a rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto;
- indicare al Presidente e Amministratore Delegato l'opportunità di emanare particolari disposizioni procedurali di attuazione dei principi contenuti nel Modello, che potrebbero non essere coerenti con quelle in vigore attualmente nella Società, curando altresì il coordinamento delle stesse con quanto esistente.
- Effettuare verifiche e controlli:
- eseguire l'attività di controllo sul rispetto delle procedure aziendali poste a presidio dei Processi Sensibili ai fini del Modello, provvedendo - se del caso - anche all'emanazione di circolari informative interne;

- condurre ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura dei Processi Sensibili;
- effettuare periodicamente verifiche mirate su determinate operazioni o specifici atti posti in essere da SEWS-Cabind, soprattutto nell'ambito dei Processi Sensibili, i cui risultati devono essere riassunti in un apposito rapporto da esporsi in sede di relazione agli organi societari deputati;
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere a lui trasmesse o tenute a sua disposizione. A tale proposito si rileva che l'Organismo di Vigilanza deve essere tempestivamente informato, da parte di tutti i dipendenti, mediante apposito sistema di comunicazione interna all'uopo predisposto dall'OdV, di quegli atti, comportamenti od eventi che possono determinare una violazione del Modello – ivi compreso eventuali segnalazioni relative alla commissione, o al ragionevole pericolo di commissione, dei reati richiamati dal D.Lgs. 231/2001 - o che, più in generale, sono rilevanti ai fini del D.Lgs. 231/2001. Oltre alle segnalazioni relative a violazioni di carattere generale sopra descritte, devono essere trasmesse all'Organismo di Vigilanza, da parte delle strutture e funzioni che operano nell'ambito dei Processi Sensibili, le informazioni riportate al successivo punto.

Nella specie le informazioni potranno riguardare, ad esempio:

- le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati previsti dalla richiamata normativa;
- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al D. Lgs. n. 231/2001;
- le relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al D. Lgs. n. 231/2001;
- le notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del Modello organizzativo, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

L'Organismo di Vigilanza dovrebbe altresì ricevere copia della reportistica periodica in materia di salute e sicurezza sul lavoro.

Va chiarito che, le informazioni fornite all'Organismo di Vigilanza mirano a consentirgli di migliorare le proprie attività di pianificazione dei controlli e non, invece, ad imporgli attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati. In altre parole all'Organismo non incombe un obbligo di agire ogni qualvolta vi sia una segnalazione, essendo rimesso alla sua discrezionalità e responsabilità di stabilire in quali casi attivarsi.

- (a) coordinarsi con le altre funzioni aziendali per il miglior monitoraggio delle attività in relazione alle procedure stabilite nel Modello. A tal fine, l'OdV ha libero accesso a tutta la documentazione aziendale che ritiene rilevante e deve essere costantemente informato dal management: a) sugli aspetti dell'attività aziendale che possono esporre SEWS-Cabind al rischio concreto di commissione di uno dei Reati; b) sui rapporti con i Consulenti e con i Partner che operano per conto della Società nell'ambito di Operazioni Sensibili;
- (b) attivare e svolgere le inchieste interne, raccordandosi di volta in volta con le funzioni aziendali interessate

per acquisire ulteriori elementi di indagine.

• **Formazione:**

- (a) coordinarsi con il Direttore del Personale per la definizione dei programmi di formazione per il personale e del contenuto delle comunicazioni periodiche da farsi ai Dipendenti e agli Organi Societari, finalizzate a fornire agli stessi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al D.Lgs. 231/2001; una volta definiti tali programmi di formazione, provvedere periodicamente alla verifica sulla qualità dei contenuti degli stessi;
- (b) predisporre ed aggiornare con continuità, nella rete aziendale, una sezione contenente tutte le informazioni relative al D.Lgs. 231/2001 e al Modello;
- (c) monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione interna necessaria al fine della sua efficace attuazione, contenente istruzioni d'uso, chiarimenti o aggiornamenti dello stesso.

• **Violazioni e sanzioni:**

- segnalare le eventuali violazioni al Modello e al D.Lgs. 231/2001 alla funzione aziendale competente, all'Amministratore Delegato ed al Direttore Risorse Umane;
- coordinarsi con l'Amministratore Delegato ed il Direttore del Personale per valutare l'adozione di eventuali sanzioni disciplinari, fermo restando la competenza di quest'ultimo per l'irrogazione della sanzione e il relativo procedimento disciplinare;
- indicare i provvedimenti più opportuni per porre rimedio alle violazioni.

Disposizione di carattere generale

In ragione dei compiti affidati, il Consiglio di Amministrazione è in ogni caso l'unico organo aziendale chiamato a svolgere un'attività di vigilanza sull'adeguatezza dell'intervento dell'OdV in quanto all'organo dirigente compete comunque la responsabilità ultima del funzionamento e dell'efficacia del Modello.

L'OdV, salva ogni diversa applicabile e prevalente disposizione di legge, ha libero accesso - senza necessità di alcun consenso preventivo - presso tutte le funzioni della Società onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal D.Lgs. 231/2001.

L'autonomia e l'indipendenza che necessariamente devono connotare le attività dell'OdV hanno reso necessario introdurre alcune forme di tutela in suo favore, al fine di garantire l'efficacia del Modello e di evitare che la sua attività di controllo possa ingenerare forme di ritorsione a suo danno (si pensi all'ipotesi in cui dagli accertamenti svolti dall'OdV possano emergere elementi che facciano risalire al massimo vertice aziendale il Reato o il tentativo di commissione del Reato o la violazione del presente Modello). Pertanto, le decisioni in merito a remunerazione, promozioni, trasferimento o sanzioni disciplinari relative ai membri dell'OdV sono attribuite alla competenza esclusiva dell'Amministratore Delegato, che dovrà acquisire obbligatoriamente il parere del Consiglio di Amministrazione.

**4.4 Attività di relazione dell'Organismo di Vigilanza verso il vertice aziendale**

L'OdV riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità. L'OdV ha due linee di attività di relazione:

- la prima, su base continuativa, direttamente verso l'Amministratore Delegato;

- la seconda, su base semestrale, verso il Consiglio di Amministrazione e il Collegio Sindacale;

In particolare, l'OdV predispone con cadenza almeno annuale un rapporto scritto per il Consiglio di Amministrazione e per il Collegio Sindacale sulla attività svolta (indicando in particolare i controlli effettuati e l'esito degli stessi, le verifiche specifiche e l'esito delle stesse, l'eventuale aggiornamento della mappatura dei Processi Sensibili, ecc.) nonché un piano annuale delle attività di verifica, controllo, e aggiornamento che saranno svolte nel corso dell'anno successivo, salvo eventuali emergenze che venissero a palesarsi.

Qualora l'OdV rilevi criticità riferibili a qualcuno dei soggetti referenti, la corrispondente segnalazione è da destinarsi prontamente agli Amministratori ed ai Sindaci.

Nel dettaglio, l'attività di relazione ha ad oggetto:

- le prestazioni svolte dall'ufficio dell'OdV;
- le eventuali criticità (e spunti per il miglioramento) emerse sia in termini di comportamenti o eventi interni a SEWS-CABIND, sia in termini di efficacia del Modello.

Gli incontri con gli organi cui l'OdV riferisce devono essere verbalizzati e copia dei verbali deve essere custodita dall'OdV e dagli Organi Sociali di volta in volta coinvolti.

Il Collegio Sindacale, il Consiglio di Amministrazione, il Presidente e l'Amministratore Delegato hanno la facoltà di convocare in qualsiasi momento l'OdV. Del pari, l'OdV ha, a sua volta, la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione dei predetti Organi Sociali per motivi urgenti.

L'OdV deve, inoltre, coordinarsi con le funzioni aziendali competenti presenti nella Società per i diversi profili specifici e precisamente:

- con la Direzione Risorse Umane, in ordine alla formazione del personale;
- con la Direzione Risorse Umane per i procedimenti disciplinari;
- con la Direzione Finanziaria, in ordine al controllo dei flussi finanziari e di tutte le attività, anche amministrative, che possono avere rilevanza ai fini della commissione dei reati societari;
- con la Direzione di stabilimento, in ordine alle attività antinfortunistiche e di tutela dell'igiene e della salute.

#### **4.5 Flussi informativi verso l'OdV: informazioni di carattere generale ed informazioni specifiche obbligatorie**

L'OdV deve essere tempestivamente informato, mediante apposite segnalazioni da parte dei Dipendenti e degli Organi Sociali in merito ad atti, comportamenti ed eventi che potrebbero ingenerare responsabilità della Società ai sensi del D.Lgs. 231/2001.

Tali segnalazioni possono essere inviate all'OdV ai seguenti indirizzi:

**Avv. Giovanni M. Marini,**  
**Presidente dell'Organismo di Vigilanza,**  
**presso Jones Day, via Turati 16/18, 20121 Milano**  
**indirizzo email: dlgs231-01@sews-cabind.it**

Valgono al riguardo le seguenti indicazioni di carattere generale:

(A) i Dipendenti e gli Organi Societari devono segnalare all'OdV le violazioni del Modello, da chiunque commesse, in particolare, le notizie relative:

- alla commissione, o al ragionevole pericolo di commissione, dei reati rilevanti ai fini della responsabilità amministrativa di SEWS-Cabind;
- a comportamenti che, in ogni caso, possono determinare una violazione del Modello;
- alle richieste di assistenza legale inoltrate a SEWS-Cabind dai Dipendenti, ai sensi del CCNL, in caso di avvio di procedimento giudiziario nei confronti degli stessi;
- ai rapporti eventualmente preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D. Lgs. 231/2001;
- alle notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i dipendenti), qualora essi siano legati a commissione di reati o violazione delle regole di comportamento o procedurali del Modello;
- alle anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (un fatto non di ripetitività o estensione dell'area di accadimento).

(B) Gli obblighi di informazione su eventuali comportamenti contrari alle disposizioni contenute nel Modello rientrano nel più ampio dovere di diligenza ed obbligo di fedeltà dei Dipendenti;

(C) L'OdV valuta le segnalazioni ricevute: l'OdV non è obbligato a prendere in considerazione le segnalazioni anonime.

(D) I segnalanti in buona fede saranno garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione ed in ogni caso sarà assicurata la riservatezza dell'identità del segnalante.

(E) Oltre alle segnalazioni relative a violazioni di carattere generale sopra descritte e sempre che si tratti di atti o fatti relativi alle attività di competenza dell'OdV, devono essere obbligatoriamente ed immediatamente trasmesse all'OdV le informazioni concernenti i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i Reati qualora tali indagini coinvolgano la Società, i Dipendenti o componenti degli Organi Sociali.

(F) L'OdV ha inoltre il potere di individuare altre informazioni che dovranno essergli trasmesse, in aggiunta a quelle sopra descritte.

#### **4.6 Raccolta e conservazione delle informazioni**

Ogni informazione, segnalazione, *report* previsto nel presente Modello è conservato dall'OdV in un apposito archivio (informatico o cartaceo) per un periodo di 10 anni. L'accesso all'archivio è consentito ai membri del Collegio Sindacale e del Consiglio di Amministrazione, salvo che non riguardino indagini nei loro confronti, nel qual caso sarà necessaria l'autorizzazione del Consiglio di Amministrazione, sentito il Collegio Sindacale e sempre che tale accesso non sia comunque garantito da norme di legge vigenti.

E' inoltre conservata a cura del personale interessato e sempre per 10 anni, la documentazione relativa a Processi

Sensibili prevista nel Modello stesso e/o dalle norme operative connesse (es.: documentazione di supporto alle “schede di evidenza” nelle operazioni sensibili).

#### **4.7 La formazione delle risorse e la diffusione del Modello**

Ai fini dell’efficacia del presente Modello, è obiettivo di SEWS-Cabind 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 in relazione al diverso livello di coinvolgimento delle risorse medesime nei Processi Sensibili.

Il sistema di informazione e formazione è supervisionato ed integrato dall’attività realizzata in questo campo dall’OdV in collaborazione con il responsabile della Direzione Risorse Umane e con i responsabili delle altre funzioni di volta in volta coinvolte nella applicazione del Modello.

L’adozione del presente Modello è comunicata dall’Amministratore Delegato a tutti i Dipendenti presenti in azienda al momento dell’adozione stessa.

Ai nuovi assunti, invece, viene consegnato materiale informativo, con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza.

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, SEWS-Cabind prevede livelli diversi di informazione e formazione attraverso idonei strumenti di diffusione, quali le comunicazioni via posta elettronica, la pubblicazione della documentazione nella rete aziendale, la partecipazione – obbligatoria per i dipendenti - a corsi di formazione e aggiornamento e altri.

### **5 SANZIONI DISCIPLINARI**

#### **5.1 Premessa**

Un punto qualificante nella costruzione del modello organizzativo è costituito dalla previsione di un sistema sanzionatorio che dia efficacia sia al codice etico che alle procedure previste dal modello stesso.

In primo luogo occorre fare una distinzione, e circoscrivere l’ambito della questione.

L’art. 6 del Decreto prevede, in modo generale, l’obbligo di “introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello”, e tale previsione vale per tutti i soggetti interessati, siano essi apicali o meno, siano dipendenti o amministratori, siano lavoratori dipendenti o autonomi.

E’ necessaria la previsione di sanzioni per gli organi sociali, specificamente gli amministratori: per loro la segnalazione al collegio sindacale, con riserva di richiesta di risarcimento dei danni, appare in effetti l’unica soluzione possibile.

Nell’ipotesi invece in cui chiamati in causa siano lavoratori subordinati, occorrerà tenere conto della complessa disciplina che caratterizza l’esercizio del potere disciplinare del datore di lavoro.

E’ quindi necessario coordinare questo tessuto normativo con le nuove disposizioni di cui al Decreto 231 del 2001.

Il punto di partenza non può che essere l’art. 7 dello Statuto dei lavoratori, norma base in materia.

E' in primo luogo necessario ricordare che da detta disposizione deriva un principio di tipicità sia delle violazioni che delle sanzioni.

Al principio di tipicità delle sanzioni si accompagna l'obbligo di dare alle fattispecie punibili un'adeguata pubblicità preventiva, mediante inclusione nel codice disciplinare ed affissione dello stesso.

A questo proposito, si è reso necessario prevedere l'affissione del documento che integra il Codice disciplinare nelle bacheche aziendali.

La figura del licenziamento per giusta causa trova la sua legittimazione ed il suo fondamento giuridico direttamente dall'art. 2119 c.c., che prevede il recesso senza preavviso "qualora si verifichi una causa che non consenta la prosecuzione, anche provvisoria, del rapporto", mentre per tutte le altre ipotesi il datore di lavoro trae il suo potere disciplinare dall'art. 7 dello Statuto dei lavoratori, ed è pertanto sottoposto a tutti i limiti e gli oneri che da tale disposizione derivano.

Nella fattispecie ora descritta possono certamente rientrare alcune tra le violazioni del codice etico, ed in particolare la commissione dei gravi reati ai quali si applica il D. lgs. 231 del 2001.

Tuttavia, per quanto riguarda le violazioni minori, per esempio la violazione degli obblighi procedurali del modello accompagnate da sanzioni conservative e dunque diverse dal licenziamento, sarà comunque necessaria la previsione da parte del codice disciplinare e la relativa pubblicità.

Un'altra questione da affrontare è quella relativa ai rapporti tra il procedimento disciplinare e l'eventuale giudizio penale vertente sugli stessi fatti.

Si deve distinguere, al riguardo, tra l'aspetto squisitamente disciplinare e l'eventuale azione di risarcimento del danno.

Mentre è comprensibile che, prima di iniziare azioni finalizzate ad ottenere il risarcimento del danno, si preferisca attendere che il giudice penale accerti con precisione ed autorevolezza i fatti, una simile attesa non sarebbe invece, salvo casi particolari, consigliabile per gli aspetti disciplinari.

E' infatti costante insegnamento della giurisprudenza la totale reciproca autonomia della valutazione del fatto effettuata dal giudice a fini penali e dal datore di lavoro a fini disciplinari.

E' superfluo precisare però che, qualora il giudice penale dovesse accertare in modo definitivo la totale insussistenza del fatto in sé posto alla base del provvedimento disciplinare, tale accertamento potrebbe riflettersi anche sulla legittimità della sanzione.

In questa ipotesi, infatti, non ci troveremmo più a discutere di differenti metri di valutazione del fatto, ma di insussistenza dello stesso.

E' chiaro che la decisione di procedere ad una sanzione, soprattutto se espulsiva, senza attendere il giudizio penale, comporta un rigorosissimo accertamento dei fatti.

Qualora sussistano dei dubbi, è opportuno servirsi dell'istituto della sospensione cautelare.

Un altro aspetto importante è quello connesso alla tempestività.

Soprattutto quando si intenda procedere ad un licenziamento per giusta causa, il cui presupposto, come si è visto, è nell'incompatibilità della violazione commessa con la prosecuzione, anche temporanea, del rapporto, attendere il giudizio penale prima di procedere può essere la prova dell'insussistenza di tale presupposto.

A questo proposito può sofferire, soprattutto quando non ci sia certezza sui fatti, l'istituto della sospensione cautelare.

La sospensione cautelare, oltre che essere opportuna nelle more del procedimento sanzionatorio di cui all'art. 7 l. 300/70 (quando l'intenzione sia di procedere ad una sanzione espulsiva), può essere utile qualora l'accertamento dei fatti che costituiscono la violazione sia particolarmente difficile, così da rendere preferibile lasciarlo ai più penetranti poteri istruttori della magistratura, senza però privarsi del potere disciplinare per mancanza di tempestività.

Venendo ad un altro punto di particolare rilievo, occorre rammentare che il sistema sanzionatorio disciplinare, come regolato nel nostro ordinamento, è caratterizzato dal principio di tipicità, oltre che delle fattispecie sanzionabili, anche delle sanzioni.

E' importante rimarcare che le sanzioni in concreto comminabili, da parte di un'impresa che applichi un contratto collettivo – come nella fattispecie - sono solo quelle espressamente previste nel CCNL stesso.

## **5.2 Misure nei confronti di quadri, impiegati ed operai - Sistema disciplinare**

La violazione, da parte dei Dipendenti soggetti al CCNL applicato in SEWS-Cabind, delle singole regole comportamentali di cui al presente Modello costituisce illecito disciplinare.

I provvedimenti disciplinari irrogabili nei riguardi di detti lavoratori - nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) - sono quelli previsti dall'apparato sanzionatorio del suddetto CCNL, e precisamente:

- . • richiamo verbale;
- . • ammonizione scritta;
- . • multa;
- . • sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni;
- . • licenziamento.

Restano ferme - e si intendono qui richiamate - tutte le previsioni previste in materia dal CCNL e relative alle procedure ed agli obblighi da osservare nell'applicazione delle sanzioni ai sensi della legge 300/1970.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, alla dirigenza aziendale.

**Il presente capitolo sarà affisso ai sensi dell'art. 7 dello Statuto dei Lavoratori unitamente CCNL.**

## **5.3 Violazioni del Modello e relative sanzioni**

Fermi restando gli obblighi per la Società nascenti dallo Statuto dei Lavoratori e dal CCNL applicato, i comportamenti sanzionabili sono i seguenti:

- a) violazione di procedure interne previste o richiamate dal presente Modello (ad esempio non osservanza delle procedure prescritte, omissione di comunicazioni all'OdV in merito a informazioni prescritte, omissione di controlli, ecc.) o adozione, nell'espletamento di attività connesse ai Processi Sensibili, di

comportamenti non conformi alle prescrizioni del Modello o alle procedure ivi richiamate;

- b) violazione di procedure interne previste o richiamate dal presente Modello o adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle prescrizioni del Modello o alle procedure ivi richiamate che espongano la Società ad una situazione oggettiva di rischio di commissione di uno dei Reati;
- c) adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle prescrizioni del presente Modello, o alle procedure ivi richiamate, e diretti in modo univoco al compimento di uno o più Reati;
- d) adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti palesemente in violazione delle prescrizioni del presente Modello, o delle procedure ivi richiamate, tali da determinare la concreta applicazione a carico della Società di sanzioni previste dal D.Lgs. 231/2001.

Le sanzioni e l'eventuale richiesta di risarcimento dei danni saranno commisurate al livello di responsabilità ed autonomia del Dipendente, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità del suo comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la Società può ragionevolmente ritenersi esposta - ai sensi e per gli effetti del D.Lgs. 231/2001 - a seguito della condotta censurata e comunque nei limiti imposti dal CCNL, Disciplina Generale, sez. terza, art. 18 "Rapporti in azienda".

Il sistema disciplinare è soggetto a costante verifica e valutazione da parte dell'OdV, e del Direttore Risorse Umane, rimanendo quest'ultimo responsabile della concreta applicazione delle misure disciplinari qui delineate su segnalazione dell'OdV e sentito, eventualmente, il superiore gerarchico dell'autore della condotta censurata.

In conformità a quanto stabilito dalla normativa rilevante e in ossequio ai principi di tipicità delle violazioni e di tipicità delle sanzioni, la Società intende portare a conoscenza dei propri dipendenti, tramite affissione le disposizioni e le regole comportamentali contenute nel Modello, la cui violazione costituisce illecito disciplinare, nonché le misure sanzionatorie applicabili, tenuto conto della gravità delle infrazioni.

Fermi restando gli obblighi in capo a SEWS-Cabind derivanti dallo Statuto dei Lavoratori, i comportamenti che costituiscono violazione del Modello, corredate dalle relative sanzioni, sono i seguenti:

1. incorre nel provvedimento di "richiamo verbale" il lavoratore che violi una delle procedure interne previste dal Modello (ad esempio, che non osservi le procedure prescritte, ometta di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, ometta di svolgere controlli, ecc.), o adotti nell'espletamento di attività nei Processi Sensibili un comportamento non conforme alle prescrizioni del Modello stesso. Tali comportamenti costituiscono una mancata osservanza delle disposizioni impartite dalla Società;
2. incorre nel provvedimento di "ammonizione scritta" il lavoratore che sia recidivo nel violare le procedure previste dal Modello o nell'adottare, nell'espletamento di attività comprese nei Processi Sensibili, un comportamento non conforme alle prescrizioni del Modello. Tali comportamenti costituiscono una ripetuta mancata osservanza delle disposizioni impartite dalla Società;
3. incorre nel provvedimento della "multa", non superiore all'importo di 3 ore della normale retribuzione, il lavoratore che nel violare le procedure interne previste dal Modello, o adottando nell'espletamento di attività nei Processi Sensibili un comportamento non conforme alle prescrizioni del Modello, esponga l'integrità dei beni aziendali ad una situazione di oggettivo pericolo. Tali comportamenti, posti in essere con la mancata osservanza delle disposizioni impartite dalla Società, determinano una situazione di pericolo per l'integrità dei beni della Società e/o costituiscono atti contrari agli interessi della stessa;
4. incorre nel provvedimento della "sospensione" dal servizio e dal trattamento retributivo per un periodo non superiore a 3 giorni il lavoratore che nel violare le procedure interne previste dal Modello, o adottando

nell'espletamento di attività nei Processi Sensibili un comportamento non conforme alle prescrizioni del Modello, arrechi danno alla Società compiendo atti contrari all'interesse della stessa, ovvero il lavoratore che sia recidivo oltre la terza volta nell'anno solare nelle mancanze di cui ai punti 1, 2 e 3. Tali comportamenti, posti in essere per la mancata osservanza delle disposizioni impartite dalla Società, determinano un danno ai beni della Società e/o costituiscono atti contrari agli interessi della stessa;

**5.** incorre nel provvedimento del “licenziamento con preavviso” (con diritto del datore di lavoro all'esonero immediato dalla attività lavorativa provvedendo alla liquidazione dei relativi emolumenti) il lavoratore che adotti, nell'espletamento delle attività nei Processi Sensibili, un comportamento non conforme alle prescrizioni del Modello e diretto in modo univoco al compimento di un reato sanzionato dal D.Lgs. 231/2001. Tale comportamento costituisce una grave inosservanza delle disposizioni impartite dalla Società e/o una grave violazione dell'obbligo del lavoratore di cooperare alla prosperità della Società;

**6.** incorre nel provvedimento del “licenziamento senza preavviso” il lavoratore che adotti nell'espletamento delle attività nei Processi Sensibili un comportamento in violazione alle prescrizioni del Modello, tale da determinare la concreta applicazione a carico della Società delle misure previste dal D.Lgs. 231/2001, nonché il lavoratore che sia recidivo oltre la terza volta nell'anno solare nelle mancanze di cui al punto 4. Tale comportamento fa venire meno radicalmente la fiducia della Società nei confronti del lavoratore, costituendo un grave nocumento morale e/o materiale per l'azienda. Ove necessario, per l'accertamento dei fatti, l'azienda si riserva di ricorrere all'istituto della sospensione cautelare.

#### **5.4 Misure nei confronti dei dirigenti**

In caso di violazione, da parte di dirigenti, delle procedure previste dal presente Modello o di adozione, nell'espletamento di attività connesse con i Processi Sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso, tra cui la violazione degli obblighi di vigilanza sui soggetti sottoposti, la Società provvede ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal CCNL per i dirigenti di aziende industriali dalla stessa applicato.

#### **5.5 Misure nei confronti degli Amministratori**

In caso di violazione del Modello da parte di uno o più membri del Consiglio di Amministrazione, l'OdV informa il Collegio Sindacale e l'intero Consiglio di Amministrazione affinché prendano gli opportuni provvedimenti. Tali provvedimenti possono consistere, a titolo esemplificativo e non esaustivo, nella revoca delle deleghe o nella sospensione o decadenza della carica.

#### **5.6 Misure nei confronti dei Sindaci**

In caso di violazione del presente Modello da parte di uno o più Sindaci, l'OdV informa l'intero Collegio Sindacale e il Consiglio di Amministrazione affinché prendano gli opportuni provvedimenti.

### **6. VERIFICHE SULL'ADEGUATEZZA DEL MODELLO**

Oltre all'attività di vigilanza che l'OdV svolge continuamente sull'effettività del Modello (e che si concreta nella verifica della coerenza tra i comportamenti concreti dei destinatari ed il Modello stesso), esso periodicamente effettua specifiche verifiche sulla reale capacità del Modello alla prevenzione dei Reati, preferibilmente coadiuvandosi con soggetti terzi in grado di assicurare una valutazione obiettiva dell'attività svolta. Tale attività si concretizza in una verifica a campione dei principali atti societari e dei contratti o atti di maggior rilevanza

conclusi o compiuti da SEWS-Cabind in relazione ai Processi Sensibili e alla conformità degli stessi alle regole di cui al presente Modello.

Le verifiche sono condotte dall'OdV che si avvale, di norma, del supporto di altre funzioni interne che, di volta in volta, si rendano a tal fine necessarie.

Le verifiche e il loro esito sono oggetto di relazione annuale al Consiglio Amministrazione e al Collegio Sindacale.

In particolare, in caso di rilevata inefficienza del Modello, l'OdV esporrà i miglioramenti da attuare.

## SEZIONE I

### I REATI NEI RAPPORTI CON LA P.A.

#### **Le fattispecie dei reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/2001)**

La presente Parte si riferisce ai reati realizzabili nell'ambito dei rapporti tra la Società e la P.A. Si indicano brevemente qui di seguito le singole fattispecie contemplate nel D.Lgs. 231/2001 agli artt. 24 e 25, rimandandosi al testo del Decreto e a quello del Codice Penale per una dettagliata descrizione delle stesse, che devono comunque intendersi già note ai sensi dell'art. 5 del Cod. Pen.

#### **1. CORRUZIONE E CONCUSSIONE**

##### **Art. 317 del codice penale (ConcuSSIONE)**

Il pubblico ufficiale o l'incaricato di un pubblico servizio, che, abusando della sua qualità o dei suoi poteri costringe o induce taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro o altra utilità, è punito con la reclusione da quattro a dodici anni.

##### **Art. 318 del codice penale (Corruzione per un atto d'ufficio)**

Il pubblico ufficiale, che, per compiere un atto del suo ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa, è punito con la reclusione da sei mesi a tre anni. Se il pubblico ufficiale riceve la retribuzione per un atto d'ufficio da lui già compiuto, la pena è della reclusione fino a un anno.

##### **Art. 319 del codice penale (Corruzione per un atto contrario ai doveri d'ufficio)**

Il pubblico ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da due a cinque anni.

##### **Art. 319-bis del codice penale (Circostanze aggravanti)**

La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene.

##### **Art. 319-ter del codice penale (Corruzione in atti giudiziari)**

Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da tre a otto anni. Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da quattro a dodici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da sei a venti anni.

##### **Art. 320 del codice penale (Corruzione di persona incaricata di un pubblico servizio)**

Le disposizioni dell'articolo 319 si applicano anche all'incaricato di un pubblico servizio; quelle di cui all'articolo 318 si applicano anche alla persona incaricata di un pubblico servizio, qualora rivesta la qualità di pubblico impiegato. In ogni caso, le pene sono ridotte in misura non superiore a un terzo.

##### **Art. 322-bis del codice penale (Peculato, concuSSIONE, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri)**

Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:

- 1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;
- 2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
- 3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
- 4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
- 5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio.

Le disposizioni degli articoli 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso:

- 1) alle persone indicate nel primo comma del presente articolo;
- 2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali.

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

**Considerazioni.** Si tratta di tipologie di reato che possono essere realizzate in molte aree aziendali ed a tutti i livelli organizzativi. Ovviamente sussistono alcuni ambiti (attività, funzioni, processi) ove il rischio si può presentare in misura maggiore.

È opportuno ricordare che la corruzione rileva anche nel caso sia realizzata nei confronti di soggetti stranieri i quali, secondo la legge italiana, siano pubblici ufficiali o incaricati di pubblico servizio.

Le ipotesi di responsabilità dell'ente per concussione sono molto più rare. Infatti, il comportamento concussivo dovrebbe rientrare tra i reati presupposto del d.lgs 231/01, essere realizzato *nell'interesse o a vantaggio* dell'ente e non, come normalmente accade, nell'esclusivo interesse del concussore.

SEWS-Cabind non svolge attività di fornitura d'opera o servizi o vendita di beni nei confronti della P.A.

Questo giustifica una prognosi di minor rischio nei confronti dei reati corruttivi.

| FATTISPECIE DI REATO  | CONTROLLI PREVENTIVI  |
|---|---|
| <ul style="list-style-type: none"><li>• Ottenere concessioni, licenze ed autorizzazioni da parte della P.A.</li><li>• Ottenere trattamenti di favore (ad esempio in sede di conciliazione amministrativa) da parte della Pubblica Amministrazione.</li><li>• Ottenere trattamenti di favore da parte di Autorità di controllo e/o di vigilanza.</li></ul> | <ul style="list-style-type: none"><li>• Esplicita previsione tra i principi etici del divieto di pratiche corruttive.</li><li>• Controllo dei flussi finanziari aziendali.</li><li>• Controllo della documentazione aziendale e, in particolare, delle fatture passive per evitare l'utilizzo di fatture per operazioni inesistenti.</li><li>• Necessità di diverse autorizzazioni durante l'iter di fatture passive, dall'ordine di acquisto al pagamento.</li></ul> |

Quanto appena descritto in tema di controlli volti a prevenire i reati di concussione e corruzione vale anche in merito ai reati di concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri previsti dall'art. 322-bis cod. pen.

## **2. TRUFFA AGGRAVATA AI DANNI DELLO STATO**

### **Art. 640 del codice penale (Truffa)**

Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1032.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1549:

1. se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare;
2. se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità.

**Considerazioni.** Si tratta di tipologie di reato realizzabili in tutti gli ambiti aziendali. È opportuno ricordare che la truffa si caratterizza per l'immutazione del vero in ordine a situazioni la cui esistenza, nei termini falsamente rappresentati, è essenziale per l'atto di disposizione patrimoniale da parte della P.A.

#### **FATTISPECIE DI REATO**

- Produzione alla P.A. di documenti falsi attestanti l'esistenza di condizioni essenziali per ottenere licenze, autorizzazioni, ecc.

#### **CONTROLLI PREVENTIVI**

- Puntuali attività di controllo gerarchico (incluso sistema di deleghe).

## **3. FRODE INFORMATICA**

### **Art. 640-ter del codice penale**

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

**Considerazioni.** È opportuno ricordare che tale fattispecie di reato assume rilievo solo se realizzata in danno della P.A. Si tratta di una tipologia di illecito la cui commissione appare poco probabile stante l'attività in concreto svolta da SEWS-Cabind. Si ricorda che il reato deve essere commesso a vantaggio o nell'interesse dell'azienda per essere rilevante ai sensi del D.Lgs.231.

## 4. REATI IN TEMA DI EROGAZIONI PUBBLICHE

### **Art. 316-bis del codice penale (Malversazione a danno dello Stato)**

Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni.

### **Art. 316-ter del codice penale (Indebita percezione di erogazioni a danno dello Stato)**

Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. Quando la somma indebitamente percepita è pari o inferiore a euro 4000 si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da 5164 a 25.822 di euro. Tale sanzione non può comunque superare il triplo del beneficio conseguito.

### **Art. 640-bis del codice penale (Truffa aggravata per il conseguimento di erogazioni pubbliche)**

La pena è della reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

**Considerazioni.** Le fattispecie richiamate mirano a tutelare l'erogazione di finanziamenti pubblici, comunque denominate, sotto due diversi profili temporali: nel momento di erogazione e nel successivo momento dell'utilizzazione dei finanziamenti. Le condotte punite, con riferimento al primo dei due momenti, sono modellate sullo schema della truffa in cui assume rilevanza determinante l'immutazione del vero in ordine ad aspetti essenziali ai fini dell'erogazione. Nella malversazione, invece, assume rilievo la mancata destinazione del finanziamento ricevuto per le finalità di interesse pubblico che ne abbiano giustificato l'erogazione.

#### **AREE AZIENDALI A RISCHIO**

- Settore finanziario
- Investimenti ambientali
- Investimenti produzione
- Ricerca ed innovazione

#### **CONTROLLI PREVENTIVI**

- Specifica previsione del codice etico.
- Diffusione del Codice Etico verso tutti i dipendenti.
- Programma di informazione/formazione periodica del dipendente.
- Struttura gerarchica atta a preservare l'ente da reati.

## **5. PROCESSI SENSIBILI NEI RAPPORTI CON LA P.A.**

I principali Processi Sensibili, che SEWS-Cabind ha individuato al proprio interno sono i seguenti:

- rapporti con Comune ed ASL in relazione all'agibilità degli uffici e dello stabilimento sito in Collegno;
- rapporti correnti con INPS e INAIL, Ispettorato del lavoro e Pubblica Sicurezza per la gestione dei rapporti di lavoro e degli eventuali infortuni sul lavoro;
- rapporti con l'Agenzia delle Entrate per questioni di carattere fiscale;
- rapporti con i vigili del fuoco ed ARPA per materie tecniche relative al funzionamento del sito di Collegno;
- rapporti con l'Ufficio delle Dogane;
- rapporti con i Ministeri competenti e la Regione Piemonte per i contributi alla formazione dei dipendenti;
- rapporti con la Prefettura per i visti dei dipendenti stranieri;
- richieste di finanziamenti e contributi pubblici;
- gestione delle ispezioni (amministrative, fiscali, previdenziali, ecc.);
- rapporti con Centro per l'Impiego per attivazione tirocini, apprendistati e rapporti con università.

### **5.1 Regole generali: l'organizzazione della Società**

In linea generale, il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

### **5.2 La struttura organizzativa**

La Società è dotata di strumenti organizzativi quali organigrammi e comunicazioni organizzative, rivolti a:

- rendere nota la struttura aziendale all'interno della Società;
- definire chiaramente e formalmente la delimitazione dei ruoli;
- dare una chiara indicazione delle linee di riporto. Inoltre, SEWS-Cabind mette a disposizione, su richiesta del proprio personale, gli organigrammi delle funzioni aziendali e le comunicazioni organizzative relative. Inoltre viene data evidenza, attraverso comunicazioni e notizie-*flash*, dei cambiamenti più importanti che interessano la struttura organizzativa.

### **5.3 Le deleghe**

Si intende per "delega" quell'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative.

I requisiti essenziali del sistema di deleghe, ai fini di una efficace prevenzione dei Reati sono i seguenti:

- le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;
- ciascuna delega deve definire in modo specifico ed inequivoco:
  - i poteri del delegato, il soggetto (organo o individuo) cui il delegato riporta gerarchicamente;

- eventualmente, gli altri soggetti ai quali le deleghe sono congiuntamente o disgiuntamente conferite;
- i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- il delegato dispone, ove necessario, di poteri di spesa adeguati alle funzioni conferitegli.

#### **5.4 Le procure**

Si intende per “procura” l'atto giuridico unilaterale con cui la Società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

I requisiti essenziali del sistema di attribuzione delle procure, ai fini di un'efficace prevenzione dei Reati sono i seguenti:

- le procure descrivono i poteri di gestione conferiti;
- la procura può essere conferita a persone fisiche espressamente individuate nella procura stessa.
- le procure indicano gli eventuali altri soggetti cui sono conferiti congiuntamente o disgiuntamente, in tutto o in parte, i medesimi poteri di cui alla procura conferita.

### **6. REGOLE GENERALI: I PRINCIPI GENERALI DI COMPORTAMENTO**

Tutte le attività, non escluse le Operazioni Sensibili, devono essere svolte conformandosi alle leggi vigenti, alle norme del Codice Etico, ai valori e alle politiche di SEWS-Cabind e alle regole contenute nel presente Modello.

I seguenti divieti di carattere generale si applicano ai Dipendenti e agli Organi Sociali della Società.

E' fatto divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 *ter* del D.Lgs. 231/2001);
- porre in essere o dare causa a violazioni dei principi e delle procedure aziendali.

#### **6.1 Nei rapporti con pubblici funzionari**

Nell'ambito dei rapporti con pubblici funzionari, siano essi rappresentanti della P.A. italiana, di pubbliche amministrazioni di altri Paesi, di organismi comunitari o internazionali, è fatto divieto di:

- effettuare o promettere elargizioni in denaro a pubblici funzionari: ai rappresentanti della P.A. o ai loro familiari non deve essere offerto o promesso, né direttamente né indirettamente, qualsiasi regalo, dono o gratuita prestazione che possa essere o, comunque, apparire connesso con il rapporto di affari con la Società o mirante ad influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società stessa. Anche in quei Paesi in cui offrire regali o doni costituisca una prassi diffusa in segno di cortesia, tali regali devono essere di natura appropriata e non contrastare con le disposizione di legge.
- accordare o promettere vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione o di loro familiari che possano determinare le stesse conseguenze previste al punto precedente; coerentemente a quanto previsto anche nel "Codice

Etico" della Società.

## **6.2 Nell'offerta di omaggi**

E' fatto divieto di distribuire o promettere omaggi e regali al di fuori di quanto previsto dalla prassi aziendale, quindi:

- eccedente le normali pratiche commerciali o di cortesia;
- o rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale.

Si ricorda che gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere benefico o culturale, o l'immagine di SEWS-Cabind. Le spese di cortesia in occasione di ricorrenze o comunque, attinenti la sfera dell'immagine e della comunicazione, sono sempre autorizzate dal Responsabile della funzione, che ne vaglia la rispondenza ai caratteri ed ai principi sopra esposti. In ogni caso, qualora sorgano dubbi in merito alla legittimità di una spesa di cortesia è opportuno sempre richiedere l'autorizzazione anche da parte dell'Amministratore Delegato.

Le liberalità di carattere benefico o culturale, ivi comprese le sponsorizzazioni, devono restare nei limiti permessi dalle relative disposizioni legali e dai principi richiamati dal Codice Etico.

In tutti i casi, regali, omaggi, spese di cortesia, liberalità e sponsorizzazioni devono essere documentati in modo adeguato per consentire le verifiche da parte dell'Organismo di Vigilanza.

## **6.3 Nel rilascio di dichiarazioni alla P.A. e nella richiesta ed utilizzo di finanziamenti pubblici**

Nell'ambito dei rapporti con la P.A. italiana, con pubbliche amministrazioni di altri Paesi, organismi comunitari o internazionali, è fatto divieto di:

- presentare dichiarazioni non veritiere al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- destinare somme ricevute da tali organismi a titolo di erogazioni, contributi o finanziamenti a scopi diversi da quelli cui erano destinati.
- 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 predisposto un apposito rendiconto sull'effettiva utilizzazione dei fondi ottenuti;
- 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 eventuali situazioni di irregolarità e anomalie.

## **7. PROCEDURE SPECIFICHE**

### **7.1 Nella gestione delle Operazioni Sensibili**

Occorre dare debita evidenza delle operazioni di:

- richiesta ed utilizzo di finanziamenti e contributi pubblici;
- comunicazione di eventuali bandi in corso;
- richiesta di autorizzazioni, licenze e brevetti, essendo queste considerate, ai fini del presente Modello, quali Operazioni Sensibili.

Inoltre, l'Organismo di Vigilanza deve essere informato, con nota scritta, di qualsiasi criticità o conflitto di interesse che sorga con la P.A.. In particolare, per ogni Operazione Sensibile:

L'Amministratore Delegato deve individuare un responsabile, solitamente coincidente con il soggetto che gestisce tale operazione e ne costituisce quindi il referente; questo “**responsabile interno**” deve mantenere traccia dell'Operazione Sensibile e riferirne all'Organismo di Vigilanza.

Nella gestione dei Processi Sensibili i destinatari del Modello devono garantire ed attestare:

1. che tutte le uscite di cassa sono avvenute a fronte: di un contratto in essere, di documentazione che attesta la avvenuta ricezione del bene o del servizio e di fattura emessa dal fornitore,
2. che le assunzioni di personale sono state effettuate a fronte di specifiche esigenze e che sono state autorizzate secondo i vigenti poteri di rappresentanza e di firma sociale;
3. che le consulenze e gli incarichi professionali sono stati assegnati a fronte di specifiche esigenze autorizzate, secondo i vigenti poteri di rappresentanza e di firma sociale e che la scelta del professionista è avvenuta secondo le disposizioni aziendali emesse in materia.

### **7.2 Nei rapporti con Consulenti e Partner**

Nell'ambito di questi rapporti, è fatto divieto di:

- effettuare prestazioni in favore dei Consulenti e dei Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- riconoscere compensi in favore dei Consulenti e dei Partner che non trovino adeguata giustificazioni in relazione al tipo di incarico da svolgere ed alla prassi vigente.

### **7.3 Nel rilascio di dichiarazioni alla P.A. e nella richiesta ed utilizzo di finanziamenti pubblici**

Nell'ambito dei rapporti con pubblici funzionari, siano essi rappresentanti della P.A. italiana, di pubbliche amministrazioni di altri Paesi, di organismi comunitari o internazionali, è fatto obbligo ai soggetti interessati di attenersi alle seguenti disposizioni:

- 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 predisposto un apposito rendiconto sull'effettiva utilizzazione dei fondi ottenuti;
- 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 eventuali situazioni di irregolarità o anomalie.

#### **7.4 Nelle ispezioni**

Per le ispezioni giudiziarie, tributarie e amministrative i referenti aziendali sono sempre almeno due e cioè il responsabile del settore ed almeno un procuratore legale con firma depositata.

Di tutto il procedimento relativo all'ispezione devono essere redatti e conservati gli appositi verbali.

L'Organismo di Vigilanza deve essere informato con nota scritta e ricevere copia del verbale da parte del responsabile della funzione coinvolta.

#### **7.5 Procedure già esistenti in SEWS-Cabind**

Le procedure rilevanti nel contesto del modello presenti in SEWS-Cabind, alle quali si rimanda, sono le seguenti:

- rispetto delle procedure per la conformità al sistema J-SOX;
- attività di *internal audit* applicate dalla capogruppo;
- le procedure di Qualità;
- le procedure di Sicurezza.
- manuale del dipendente;

Caratteristica comune alle citate procedure è il coinvolgimento di più enti e referenti aziendali.

### **8. CONTROLLI DELL'ORGANISMO DI VIGILANZA**

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività connesse ai Processi Sensibili diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello.

In particolare, l'OdV verifica periodicamente, con il supporto delle altre funzioni competenti:

- il sistema di deleghe e procure in vigore e della loro coerenza con tutto il sistema delle comunicazioni organizzative (tali sono quei documenti interni all'azienda con cui vengono conferite le deleghe), raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie;
- le Operazioni Sensibili in corso;
- le liberalità effettuate;
- i rapporti in corso con terzi, in particolar modo con i consulenti. In ragione dell'attività di vigilanza attribuita all'OdV nel presente Modello, a tale organismo viene garantito libero accesso a tutta la documentazione aziendale che lo stesso ritiene rilevante al fine del monitoraggio dei Processi Sensibili individuati nella presente Sezione;
- I verbali redatti a seguito di ispezioni.

## **SEZIONE II**

### **REATI SOCIETARI**

#### **Le fattispecie dei reati societari (art. 25 ter del D.Lgs.231/2001)**

La presente SEZIONE si riferisce ai reati societari. Si indicano brevemente qui di seguito le singole fattispecie contemplate nel D.Lgs. 231/2001 all'art. 25-ter, rimandandosi al testo del Decreto e a quello del Codice Penale o del Codice Civile per una dettagliata descrizione delle stesse, che devono comunque intendersi già note ai sensi dell'art. 5 del Cod. Pen.

Si precisa che non essendo i titoli di SEWS-Cabind direttamente quotati in mercati regolamentati italiani o di altro Stato dell'UE o diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 TU 58/1998 e successive modificazioni e, non essendo SEWS-Cabind soggetto sottoposto a vigilanza, non si sono esaminati i reati esclusivi delle società che presentano queste caratteristiche.

#### **1. REATI SOCIETARI**

Il D. Lgs. n. 61/2002 ha introdotto la previsione di sanzioni pecuniarie a carico dell'ente in caso di commissione di reati societari.

Il decreto in oggetto ha previsto, infatti, l'inserimento nel D. Lgs. n. 231/2001 dell'art. 25-ter (Reati societari), che introduce specifiche sanzioni a carico della società "in relazione a reati in materia societaria previsti dal codice civile, se commessi nell'interesse della società da amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si sarebbe realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica". Ancorché il testo di tale articolo non menzioni esplicitamente i due elementi che caratterizzano il D. Lgs. n. 231/2001 - il "Modello di organizzazione, gestione e controllo" e l'"Organismo di vigilanza" - il riferimento ad essi può ritenersi implicito per effetto dell'inquadramento della norma nella disciplina citata. Inoltre, anche a prescindere da un'espressa previsione normativa, la loro predisposizione, oltre ad assumere in sede processuale un'importante valenza probatoria della volontà dell'ente di eliminare i difetti di organizzazione che possano facilitare la commissione di determinati illeciti, può effettivamente assicurare un'accresciuta trasparenza delle procedure e dei processi interni all'impresa e, quindi, maggiori possibilità di controllo dell'operato dei manager.

Da ciò nasce dunque la duplice esigenza di: a) approntare specifiche misure organizzative e procedurali atte a fornire ragionevole garanzia di prevenzione di questa tipologia di reati; b) precisare i compiti principali dell'Organismo di vigilanza per assicurare l'effettivo, efficace, efficiente e continuo funzionamento del modello stesso.

E' opportuno precisare che una maggiore attenzione è stata dedicata ai primi due reati disciplinati dall'art. 25-ter (art. 2621 - False comunicazioni sociali e art. 2622 - False comunicazioni sociali in danno della società, dei soci e dei creditori) poiché si riferiscono, fra l'altro, al bilancio annuale ed a quelli infrannuali che rappresentano indubbiamente i documenti più complessi, che più facilmente si prestano a "manipolazioni".

Si evidenzia che SEWS-Cabind sottopone il bilancio a certificazione volontaria .

Si evidenzia, inoltre, che SEWS-Cabind è conforme al sistema J-SOX.

La capogruppo *Sumitomo Electric Industries Limited* è quotata in Giappone. La capogruppo effettua attività di

*internal audit* alle proprie principali controllate, compresa SEWS-Cabind.

## **2. FUNZIONI DELLA SEZIONE II**

La presente Parte si riferisce a comportamenti posti in essere dai Dipendenti e dagli Organi Sociali di SEWS-Cabind.

Obiettivo della presente Parte è che tutti i destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi dei Reati in essa considerati.

Nello specifico, la presente sezione ha lo scopo di:

- indicare le procedure che i Dipendenti e gli Organi Sociali di SEWS-Cabind sono chiamati ad osservare per una corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza e ai responsabili delle altre funzioni aziendali che con lo stesso cooperano, gli strumenti esecutivi per esercitare le previste attività di controllo, monitoraggio e verifica.

## **3. PROCESSI SENSIBILI NELL'AMBITO DEI REATI SOCIETARI**

I principali Processi Sensibili, che SEWS-Cabind ha individuato al proprio interno, sono i seguenti:

- formazione del bilancio e predisposizione delle comunicazioni a soci e/o a terzi relative alla situazione economica, patrimoniale e finanziaria della Società;
- operazioni relative al capitale sociale;
- gestione dei rapporti con gli organi di controllo (Società di revisione contabile, Collegio Sindacale, ecc.) e formazione della volontà assembleare;
- rapporti con le società controllate in Polonia (*SEWS-Cabind Poland Sp.zo.o.*) e Marocco (*SEWS-Cabind Maroc SA*);
- redazione del bilancio consolidato con le società controllate.

## **4. REGOLE GENERALI**

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, gli Organi Sociali di SEWS-Cabind (e i suoi Dipendenti, nella misura necessaria alle funzioni dagli stessi svolte) devono in generale conoscere e rispettare:

- il sistema di controllo interno e quindi le procedure SEWS-Cabind, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale ed organizzativa ed il sistema di controllo di gestione;
- il Codice Etico;
- il sistema amministrativo, contabile, finanziario e di attività di relazione.
- il sistema di comunicazione al personale e di formazione dello stesso;
- il sistema disciplinare di cui ai CCNL;
- in generale, la normativa italiana e straniera applicabile;

- le regole di cui alla Parte Generale del presente Modello;
- le regole e le procedure per i singoli Processi Sensibili, come di seguito descritte in questa Sezione.

## **5. PRINCIPI DI COMPORTAMENTO E PROCEDURE SPECIFICHE**

La presente SEZIONE prevede l'espresso divieto a carico degli Organi Sociali di SEWS-Cabind (e dei suoi Dipendenti, Consulenti e Partner nella misura necessaria alle funzioni dagli stessi svolte) di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 *ter* del D.Lgs. 231/2001);
- porre in essere o dare causa a violazioni dei principi e delle procedure aziendali.

### **5.1 Formazione del bilancio e predisposizione delle comunicazioni ai soci e/o ai terzi relative alla situazione economica, patrimoniale e finanziaria della Società**

La presente SEZIONE prevede l'espresso obbligo a carico degli Organi Sociali di SEWS-Cabind (e dei suoi Dipendenti nella misura necessaria alle funzioni dagli stessi svolte) di:

**tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società.**

E' fatto divieto di:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- alterare i dati e le informazioni finalizzate alla formazione del bilancio;
- illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della Società.

Allo scopo di prevenire i comportamenti sopra elencati, sono stati creati i seguenti presidi anche nel rispetto del sistema J-SOX:

- norme che definiscono con chiarezza, per il personale coinvolto in attività di predisposizione del bilancio, i principi contabili da adottare per la definizione delle poste del bilancio e le modalità operative per la loro contabilizzazione. Tali norme sono aggiornate dagli uffici competenti alla luce delle novità della normativa fiscale e civilistica e diffuse ai destinatari sopra indicati;
- istruzioni rivolte ai servizi e alle funzioni della Società, che indichino dati e notizie che queste devono fornire ai servizi coinvolti nel processo di redazione del bilancio in relazione alle chiusure annuali ed infrannuali, nonché le relative modalità e la tempistica;
- un sistema informatico per la trasmissione di dati e informazioni che garantisca la tracciabilità dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema. Il

responsabile di ciascun servizio coinvolto nel processo garantisce inoltre la tracciabilità delle informazioni contabili non generate in automatico dal sistema;

- regole per la tenuta, conservazione e aggiornamento dei fascicoli relativi ai bilanci, dalla loro approvazione da parte del Consiglio di Amministrazione al deposito e pubblicazione (anche informatica) degli stessi fino alla relativa archiviazione.
- effettuazione di uno o più incontri fra il Collegio Sindacale e la Società di revisione per lo scambio di informazioni sulle attività di revisione (art. 2409 *septies* c.c.);
- effettuazione di una o più riunioni, tra l'Organismo di Vigilanza e la Società di revisione per la valutazione di eventuali criticità emerse nello svolgimento delle attività di revisione.

## **5.2 Operazioni relative al capitale sociale**

La presente SEZIONE prevede l'espresso obbligo a carico degli Organi Sociali di SEWS-Cabind (e dei suoi Dipendenti, Consulenti e Partner nella misura necessaria alle funzioni dagli stessi svolte) di:

**osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere.**

In particolare, è fatto divieto di:

- restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi previsti dalla legge;
- ripartire utili non effettivamente conseguiti o destinati per legge a riserva;
- acquistare o sottoscrivere azioni fuori dai casi previsti dalla legge;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione alle disposizioni di legge a tutela dei creditori;
- procedere a formazione o aumento fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;
- procedere a operazioni sul capitale sociale di SEWS-Cabind, costituire società, acquisire e cedere partecipazioni, effettuare fusioni e scissioni al di fuori delle procedure aziendali all'uopo predisposte.

Allo scopo di prevenire i comportamenti sopra elencati, sono stati creati i seguenti presidi:

- relazione per il Consiglio di Amministrazione che giustifica la distribuzione di utili e riserve nel rispetto di quanto previsto dalla legge.
- adeguata giustificazione, documentazione e relativa archiviazione di eventuali modifiche apportate alla bozza di bilancio/situazioni infrannuali da parte del Consiglio Amministrazione con particolare riferimento agli utili ed alle riserve.
- adeguata giustificazione tramite documenti e relativa archiviazione di eventuali operazioni sul capitale sociale di SEWS-Cabind e operazioni di costituzione società, acquisizione e cessione. Comunicazione della decisione.

### **5.3 Gestione dei rapporti con gli organi di controllo e formazione della volontà assembleare**

La presente SEZIONE prevede l'espresso obbligo a carico degli Organi Sociali di SEWS-Cabind (e dei suoi Dipendenti, Consulenti e Partner nella misura necessaria alle funzioni dagli stessi svolte) di:

**assicurare il regolare funzionamento della Società, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;**

In particolare, è fatto divieto di:

- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del Collegio Sindacale o della Società di revisione, in violazione delle direttive che sanciscano l'obbligo alla massima collaborazione e trasparenza nei rapporti con Collegio Sindacale e Società di revisione;
- determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- attribuire gli incarichi di consulenza, aventi ad oggetto attività diversa dalla revisione contabile, alla medesima società di revisione, o alle società o entità professionali facenti parte del medesimo gruppo della società di revisione.

**Art. 2621 del codice civile**

### **6. FALSE COMUNICAZIONI SOCIALI – FALSE COMUNICAZIONI SOCIALI IN DANNO DELLA SOCIETÀ, DEI SOCI E DEI CREDITORI**

Salvo quanto previsto dall'articolo 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazioni ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, sono puniti con l'arresto fino a due anni. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi. La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento. In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta.

Nei casi previsti dai commi terzo e quarto, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa.

## Art. 2622 del codice civile

Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sè o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, esponendo fatti materiali non rispondenti al vero ancorché oggetto di valutazioni, ovvero omettendo informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, cagionano un danno patrimoniale alla società, ai soci o ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Si procede a querela anche se il fatto integra altro delitto, ancorché aggravato, a danno del patrimonio di soggetti diversi dai soci e dai creditori, salvo che sia commesso in danno dello Stato, di altri enti pubblici o delle Comunità europee. Nel caso di società soggette alle disposizioni della parte IV, titolo III, capo II, del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, la pena per i fatti previsti al primo comma è da uno a quattro anni e il delitto è procedibile d'ufficio. La pena è da due a sei anni se, nelle ipotesi di cui al terzo comma, il fatto cagiona un grave nocumento ai risparmiatori. Il nocumento si considera grave quando abbia riguardato un numero di risparmiatori superiore allo 0,1 per mille della popolazione risultante dall'ultimo censimento ISTAT ovvero se sia consistito nella distruzione o riduzione del valore di titoli di entità complessiva superiore allo 0,1 per mille del prodotto interno lordo. La punibilità per i fatti previsti dal primo e terzo comma è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi. La punibilità per i fatti previsti dal primo e terzo comma è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento. In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 per cento da quella corretta.

Nei casi previsti dai commi settimo e ottavo, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa.

**Considerazioni.** La legge 28 dicembre 2005, n. 262, recante "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari" ha apportato numerose modifiche alla disciplina dei reati di false comunicazioni sociali e di falso in prospetto. Quanto alla disciplina delle false comunicazioni sociali, le novità introdotte con la legge 262/2005 e successive modificazioni possono essere così sintetizzate. Con riguardo alla fattispecie di reato contravvenzionale, disciplinata dall'art. 2621, è stata aumentata fino a due anni la sanzione dell'arresto (la sanzione precedentemente prevista era l'arresto fino ad un anno e sei mesi). Sempre in relazione all'art. 2621, sono state introdotte sanzioni amministrative pecuniarie a carico delle persone fisiche autrici del reato, nonché sanzioni interdittive. In particolare, l'ultimo comma della norma prevede l'applicazione della sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa. La norma non chiarisce tuttavia il valore delle quote. Per quel che attiene invece all'art. 2622, l'aumento della sanzione riguarda soltanto le società con titoli quotati e, pertanto, non riguarda SEWS-Cabind.

Infine, anche con riferimento alla fattispecie di reato di cui al 2622, sono state introdotte sanzioni amministrative pecuniarie, nonché sanzioni interdittive. In particolare, l'ultimo comma stabilisce che, ai soggetti di cui al primo

comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa.

Un'ulteriore riflessione va fatta circa il livello al quale possono commettersi i reati in esame. È evidente che questi reati saranno commessi il più delle volte da chi formalmente è responsabile di questi documenti e cioè il Consiglio di Amministrazione nella sua collegialità che, ai sensi dell'art. 2423 cod. civ., redige il bilancio, la nota integrativa e la relazione sulla gestione. Al riguardo va però tenuto presente che, spesso, il Consiglio non ha né il tempo né gli strumenti per approfondire nei minimi dettagli la correttezza del gran numero di valori e note esplicative che il bilancio contiene e si affida all'operato di quello (o quelli), tra i suoi componenti, con deleghe operative. Inoltre, va sottolineato che è possibile che tali reati siano posti in essere dai livelli sottostanti, segnatamente dai responsabili delle varie funzioni aziendali. Ancora, è altresì possibile che reati di questo genere siano commessi da "sottoposti" dei responsabili di funzione, dotati di un certo potere discrezionale ancorché circoscritto. In tali casi il reato potrà dirsi consumato solo se la falsità sia consapevolmente condivisa dai soggetti "qualificati" (amministratori, ecc.) che nel recepire il dato falso lo fanno proprio inserendolo nella comunicazione sociale. Se non vi è tale partecipazione cosciente e volontaria da parte dei soggetti "qualificati" non solo tali soggetti non potranno essere ritenuti responsabili, ma, altresì, il reato non sarà configurabile. Infatti trattandosi di reati "propri" è indispensabile quantomeno la partecipazione di un soggetto provvisto della qualifica soggettiva voluta dalla legge. Peraltro l'esperienza insegna che le falsità commesse dai "subalterni" vengono realizzate nell'interesse esclusivo degli stessi (per esempio per coprire un ammanco di cassa) e ben difficilmente nell'interesse dell'ente. Ciò esclude, come è noto, ogni responsabilità ai sensi della legge di cui ci occupiamo. Nel caso, invece più frequente, di falsità realizzata dal subordinato su indicazione, ad esempio, dell'amministratore (si pensi al caso di valutazioni mendaci di crediti o partecipazioni, realizzate nell'interesse della società) la responsabilità dell'ente non potrà escludersi.

Ciò non di meno un modello di organizzazione, gestione e controllo avente l'obiettivo di impedire - con ragionevole certezza - la commissione di questa tipologia di reati, deve prendere in considerazione tutte le ipotesi appena descritte circa i possibili esecutori materiali del reato, nonché l'intero processo che porta alla formazione dei documenti qui considerati, sino alla loro sottoposizione all'Assemblea dei soci e prevedere specifici meccanismi, procedure e protocolli di prevenzione e controllo.

Nonostante SEWS-Cabind sottoponga il bilancio a certificazione volontaria da parte di una società di revisione, sarebbe tuttavia azzardato ritenere che, solo per questo, il modello possa essere ridotto ai minimi termini: infatti, reati della specie in esame possono verificarsi anche in società assoggettati a revisione e certificazione del bilancio. In questi casi, pure se emergessero responsabilità a carico del revisore, il Giudice potrebbe far scattare anche le sanzioni ex D. Lgs. n. 231/2001, una volta accertato che il "modello" non era adeguato o non era rispettato.

Quanto, poi, all'Organismo di vigilanza, i compiti di vigilare sul funzionamento e l'osservanza del modello, con riferimento ai reati in esame, potranno essere più o meno vasti in relazione, anche in questo caso, alla presenza o meno dell'istituto della certificazione del bilancio; ma non potranno mai essere azzerati nel presupposto che i controlli dei revisori esterni rendano superflua l'azione dell'OdV. Al contrario, può essere opportuno introdurre controlli ad hoc sull'operato del revisore, soprattutto in termini di mantenimento di quell'indipendenza, senza la quale la certificazione rischia di risultare un mero timbro formale sui documenti predisposti dall'ente.

## FATTISPECIE DI REATO

L'Amministratore Delegato (o il Liquidatore o il Direttore Generale) ignora l'indicazione del Responsabile Amministrativo circa l'esigenza di un accantonamento (rettifica) al Fondo svalutazione crediti a fronte della situazione i crisi di un cliente, ed iscrive un ammontare di crediti superiore al dovuto; ciò al fine di non far emergere una perdita che comporterebbe l'assunzione di provvedimenti sul capitale sociale (artt. 2446 e 2447 cod. civ.).

## CONTROLLI PREVENTIVI (PROTOCOLLI) E PRINCIPALI ATTIVITÀ DELL'OdV

1. Inserimento nel Codice etico adottato dall'impresa di specifiche previsioni riguardanti il corretto comportamento di tutti i dipendenti coinvolti nelle attività di formazione del bilancio o di altri documenti simili. Ad esempio: massima collaborazione; completezza e chiarezza delle informazioni fornite; accuratezza dei dati e delle elaborazioni; segnalazione di conflitti di interesse; ecc.

2. Attività di formazione di base verso tutti responsabili di funzione, affinché conoscano almeno le principali nozioni sul bilancio (norme di legge, sanzioni, principi contabili, ecc.).

3. Obbligo – per il Responsabile di funzione che fornisce dati ed informazioni relative al bilancio o ad altre comunicazioni sociali - di sottoscrivere una dichiarazione di veridicità e completezza delle informazioni trasmesse.

4. Tempestiva messa a disposizione di tutti i componenti del CdA della bozza del bilancio, prima della riunione del CdA per l'approvazione dello stesso; il tutto con una documentata certificazione dell'avvenuta consegna della bozza in questione.

5. Messa a disposizione delle persone *sub* 4 del giudizio sul bilancio (o attestazione similare, sufficientemente chiara ed analitica) da parte della società di certificazione.

6. Sottoscrizione, da parte del massimo Vertice Esecutivo, della c.d. lettera di attestazione o di manleva richiesta dalla società di revisione. La lettera deve essere altresì siglata dal Responsabile amministrativo e messa a disposizione dei membri del CdA. Occorre precisare tuttavia che tale lettera non elimina di per sé la responsabilità della società di revisione.

7. Procedura che preveda almeno una riunione tra la società di certificazione; il Collegio Sindacale e l'OdV prima della seduta del Consiglio di Amministrazione indetta per l'approvazione del bilancio, che abbia per oggetto tale documento, con relativa stesura di verbale.

8. Comunicazione sistematica all'OdV di qualsiasi incarico conferito, o che si intende conferire, alla società di revisione (se esistente) o a società ad essa collegate, diverso da quello concernente la certificazione del bilancio.

9. Invio all'OdV delle valutazioni in ordine alla scelta della

società di revisione (in base ad elementi quali professionalità, esperienza nel settore, ecc. e non solo in base all'economicità). I risultati dell'attività dell'OdV devono essere riportati, in via normale, al massimo Vertice esecutivo.

Peraltro, nel caso in cui dagli accertamenti svolti dal citato Organismo emergessero elementi che fanno risalire il reato (o il tentativo di commissione del reato) proprio al massimo Vertice esecutivo, sarà inevitabile che l'Organismo riferisca al Consiglio di Amministrazione e/o al Collegio sindacale.

## **7 IMPEDITO CONTROLLO - ART. 2625 DEL CODICE CIVILE**

Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali o alle società di revisione, sono puniti con la sanzione amministrativa pecuniaria fino a 10.329 Euro.

Se la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa.

La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

**Considerazioni.** Il reato in oggetto è trattato nel presente modello esclusivamente riguardo alla fattispecie prevista dal secondo comma che, sola, può comportare una responsabilità ex D. Lgs. n. 231/2001. Infatti, nel caso previsto dal primo comma la condotta, seppur sostanzialmente identica non integra reato, essendo prevista soltanto una sanzione amministrativa. Si ribadisce, ancora una volta, che il fatto deve essere realizzato nell'interesse della società e non, ad esempio, di amministratori o di una parte della compagine societaria.

## **8. ILLECITA INFLUENZA SULL'ASSEMBLEA - ART. 2636 DEL CODICE CIVILE**

Chiunque, con atti simulati o fraudolenti determina la maggioranza in assemblea allo scopo di procurare a sé o ad altri un ingiusto profitto è punito con la reclusione da sei mesi a tre anni.

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

## **9. AGGIOTAGGIO - ART. 2637 DEL CODICE CIVILE**

Chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari è punito con la pena della reclusione da uno a cinque anni.

**Considerazioni.** Si ritiene estremamente improbabile la commissione di tale reato nella fattispecie.

## **10. ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE - ART. 2628 DEL CODICE CIVILE.**

Gli amministratori che, 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, sono puniti con la reclusione fino ad un anno. La stessa pena si applica agli amministratori che, 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. 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, il reato è estinto.

**Considerazioni.** Si ritiene estremamente improbabile la commissione di tale reato nella fattispecie.

## **11. OPERAZIONI IN PREGIUDIZIO DEI CREDITORI - ART. 2629 DEL CODICE CIVILE.**

Gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Ai fini della configurabilità del reato è necessario che alla condotta in violazione delle norme civilistiche che governano le operazioni descritte sia consequenzialmente connesso "il danno ai creditori". Ancora maggiore evidenza acquista la rilevanza "privatistica" della fattispecie penale se si considera che la stessa è accompagnata dalla previsione della procedibilità a querela del danneggiato nonché da una causa di estinzione del reato costituita dal "risarcimento del danno ai creditori prima del giudizio".

Siamo ancora dinanzi ad un'ipotesi di condotta "dolosa" ed anche in questo caso è possibile l'attribuzione di responsabilità anche a titolo di "dolo eventuale", costituita dalla intenzionalità di violare le disposizioni che presiedono al corretto svolgimento delle operazioni di riduzione del capitale sociale, fusione e scissione societaria, accompagnata dalla mera accettazione della possibilità che l'evento del danno ai creditori si verifichi. Si tratta di un reato "proprio" che può essere commesso solo dagli amministratori.

### **CONTROLLI PREVENTIVI**

- Specifica previsione del Codice Etico.
- Diffusione del Codice Etico nel contesto dell'intera organizzazione aziendale.
- Programma di informazione/formazione periodica degli amministratori, del management e dei dipendenti sulla normativa di *Corporate Governance* e sui reati/illeciti amministrativi in materia societaria.
- Esistenza di un sistema definito di responsabilità del Vertice aziendale e di deleghe coerenti con esso.
- Istituzioni di riunioni periodiche tra Collegio Sindacale ed Organismo di Vigilanza anche per verificare l'osservanza della disciplina prevista in tema di normativa societaria/*Corporate Governance*, nonché il rispetto dei comportamenti conseguenti da parte degli Amministratori, del *Management* e dei dipendenti.

- Previsione di un sistema sanzionatorio interno aziendale.

### **I controlli dell'Organismo di Vigilanza**

L'OdV effettua periodicamente controlli a campione sulle attività sociali potenzialmente a rischio di reati societari, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, particolare, alle procedure interne in essere.

In ragione dell'attività di vigilanza attribuita all'OdV nel presente Modello, a tale organismo viene garantito in generale libero accesso a tutta la documentazione aziendale che lo stesso ritiene rilevante al fine del monitoraggio dei Processi Sensibili individuati nella presente SEZIONE.

## SEZIONE III

### REATI DI CRIMINALITÀ INFORMATICA

La 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” ha ampliato le fattispecie di reato che possono generare la responsabilità dell’ente, introducendo, nel corpo del D. Lgs. n. 231/2001, l’art. 24-bis “Delitti informatici e trattamento illecito di dati”.

I nuovi reati “presupposto” della responsabilità amministrativa degli enti introdotti dalla l. n. 48/2008 sono i seguenti:

#### **Art. 491-bis. del codice penale** (Documenti informatici)

*Se alcuna delle falsità previste dal presente capo 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.*

#### **Art. 615 ter del codice penale** (Accesso abusivo ad un sistema informatico o telematico)

*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza*

*ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:*

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

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

*3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.*

#### **Art. 615 quater del codice penale** (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)

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

#### **Art. 615-quinquies del codice penale** (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)

*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 del codice penale** (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)

*Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:*

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

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

*3) da chi esercita anche abusivamente la professione di investigatore privato.*

**Art. 617-quinquies del codice penale** (Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche)

*Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater.*

**Art. 635-bis del codice penale** (Danneggiamento di informazioni, dati e programmi informatici)

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

*Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635<sup>1</sup> 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 del codice penale** (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità)

*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. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.*

**Art. 635-quater del codice penale** (Danneggiamento di sistemi informatici o telematici)

*Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in*

*tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.*

**Art. 635-quinquies del codice penale** (Danneggiamento di sistemi informatici o telematici di pubblica utilità)

*Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.*

**Art. 640-quinquies del codice penale** (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*

#### **Sanzioni a carico dell'ente**

In caso di commissione di reati informatici, le sanzioni applicabili alle aziende/enti possono essere di natura pecuniaria ed interdittiva e variano a seconda della fattispecie criminosa realizzata:

| REATO PRESUPPOSTO   | SANZIONE PECUNIARIA              | SANZIONI INTERDITTIVE  |
|---|----------------------------------|--|
| <p>Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)</p> <p>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)</p> <p>Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)</p> <p>Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)</p> <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.)</p> <p>Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)</p> <p>Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)</p> | <p><b>Da 100 a 500 quote</b></p> | <p>Interdizione dall'esercizio dell'attività;</p> <p>Sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;</p> <p>Divieto di pubblicizzare beni o servizi.</p> |

| REATO PRESUPPOSTO  | SANZIONE PECUNIARIA   | SANZIONI INTERDITTIVE   |
|--|---|---|
| <p>Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)</p> <p>Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)</p> | <p><b>Fino a 300 quote</b></p>  | <p>Sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;</p> <p>Divieto di pubblicizzare beni o servizi.</p>  |
| <p>Falsità in un documento informatico pubblico o privato avente efficacia probatoria (art. 491 bis c.p.)</p> <p>Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)</p>  | <p><b>Fino a 400 quote</b><br/>(salvo quanto previsto dall'articolo 24 del D.Lgs. 231/2001 per i casi di frode informatica in danno dello Stato o di altro ente pubblico)</p> | <p>Divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;</p> <p>Esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;</p> <p>Divieto di pubblicizzare beni o servizi.</p> |

### Considerazioni generali

Il nuovo articolo 24-bis del D. Lgs. n. 231/2001 ha esteso la responsabilità amministrativa delle persone giuridiche e degli enti alla quasi totalità dei reati informatici.

Alla luce dei presupposti applicativi del decreto, la Società sarà considerata responsabile per i delitti informatici commessi nel suo interesse o a suo vantaggio da persone che rivestono funzioni di rappresentanza, amministrazione, direzione dell'ente o di una sua unità organizzativa, ma anche da persone sottoposte alla loro direzione o vigilanza.

Le tipologie di reato informatico, quindi, interessano quei comportamenti illeciti posti in essere dai soggetti in posizione apicale o subordinata (dipendenti e/o collaboratori), che utilizzano gli strumenti e le tecnologie informatiche/telematiche aziendali per lo svolgimento delle normali attività lavorative.

Non essendo SEWS-Cabind una società che utilizza in maniera preponderante gli strumenti informatici e telematici per lo svolgimento delle proprie attività e per l'erogazione di servizi, la essa è evidentemente in minor misura esposta ai suddetti comportamenti illeciti.

E' comunque opportuno che siano implementate idonee strategie preventive atte ad impedire la realizzazione dei reati informatici e ad escludere la responsabilità dell'azienda nel caso di commissione dei reati. In questo scenario, nasce l'esigenza di effettuare controlli e verifiche periodiche specialmente in quelle aree aziendali (es. gestione finanziaria, gestione clienti/fornitori, area ICT, ecc.) maggiormente esposte al rischio di commissione di reati informatici che possano determinare un interesse o un vantaggio economico per l'azienda.

SEWS-Cabind ha adottato delle Direttive generali e politiche in materia di infrastrutture informatiche volte ad evitare la commissione dei reati informatici.

SEWS-Cabind rispetta tutte le disposizioni del codice in materia di protezione dei dati personali - D. Lgs. n. 196/2003 e della Legge 300/1970 Statuto dei Lavoratori.

SEWS-Cabind è soggetta ad *audit* periodici da parte degli enti certificatori e da parte della capogruppo giapponese.

| FATTISPECIE DI REATO   | CASISTICHE  | CONTROLLI PREVENTIVI   |
|--|---|--|
| <p><b>Falsità in un documento informatico pubblico o privato avente efficacia probatoria (art. 491-bis c.p.)</b></p> | <p>Falsificazione di documenti informatici da parte di enti che procedono a rendicontazione elettronica di attività</p> <p>Cancellazione o alterazione di informazioni a valenza probatoria presenti sui propri sistemi, allo scopo di eliminare le prove di un altro reato (es. l'ente ha ricevuto un avviso di garanzia per un reato e procede ad eliminare le tracce elettroniche del reato stesso)</p> <p>Falsificazione di documenti informatici contenenti gli importi dovuti dall'ente alla PA nel caso di flussi informatizzati dei pagamenti tra privati e PA (es. riduzione degli importi) o alterazione dei documenti in transito nell'ambito del SIPA (Sistema Informatizzato pagamenti della PA) al fine di aumentare gli importi dovuti dalla PA all'ente</p> <p>Falsificazione di documenti informatici compiuta nell'ambito dei servizi di <i>Certification Authority</i> da parte di un soggetto che rilasci certificati informatici, aventi valenza probatoria, corrispondenti a false identità o attestanti falsi titoli professionali</p> <p>Falsificazione di documenti informatici correlata all'utilizzo illecito di dati identificativi altrui nell'esecuzione di determinate operazioni informatiche o telematiche in modo che queste risultino eseguite dai soggetti legittimi titolari dei dati (es. attivazione di servizi non richiesti)</p> | <p>Oltre ai controlli generali sopra citati, sono applicati i seguenti controlli specifici:</p> <ul style="list-style-type: none"> <li>• misure di protezione dell'integrità delle informazioni messe a disposizione su un sistema accessibile al pubblico, al fine di prevenire modifiche non autorizzate;</li> <li>• misure di protezione dei documenti elettronici (es. firma digitale);</li> <li>• procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme a disposizioni di legge e contrattuali.</li> </ul> |

| FATTISPECIE DI REATO   | CASISTICHE  | CONTROLLI PREVENTIVI   |
|--|---|--|
| <p><b>Accesso abusivo ad un sistema informatico o telematico<sup>2</sup></b><br/>(art. 615-ter c.p.)</p> | <p>Violazione dei sistemi informatici dei concorrenti per acquisire a scopo di spionaggio industriale la documentazione relativa ai loro prodotti/progetti. Tale condotta assume particolare rilievo per gli enti la cui attività è basata su brevetti/disegni/attività di R&amp;S (es. <i>automotive, design, moda, tecnologie, ecc.</i>).</p> <p>Accesso abusivo a sistemi <i>target</i> (di concorrenti o di enti presso i quali si suppone siano registrate determinate informazioni) allo scopo di acquisire informazioni (es. costi di produzione del cliente) utili a elaborare e implementare strategie di <i>marketing</i> o altro (es. <i>recruiting, ecc.</i>).</p> <p>Accesso abusivo a sistemi interbancari al fine di modificare le informazioni sul proprio conto registrate su tali sistemi.</p> <p>Manipolazione di dati presenti sui propri sistemi come risultato dei processi di <i>business</i> allo scopo di produrre un bilancio falso.</p> <p>Accesso abusivo a sistemi aziendali protetti da misure di sicurezza, da parte di utenti dei sistemi stessi, per attivare servizi non richiesti dalla clientela.</p> <p>Accesso abusivo ai sistemi che realizzano la fatturazione dei servizi ai clienti per alterare le informazioni e i programmi al fine di realizzare un profitto illecito.</p> <p>Accesso abusivo ai sistemi che elaborano le buste paghe per alterare i dati relativi alle voci di cedolino al fine di ridurre illecitamente le erogazioni nei confronti degli stessi e realizzare così un interesse o un vantaggio per l'ente.</p> <p>Accesso abusivo ai sistemi che gestiscono il credito di clienti di servizi pre-pagati per modificare i dati di credito e realizzare un profitto per l'ente (come ad esempio avviene nei settori delle telecomunicazioni).</p> | <p>L'accesso abusivo, oltre ad essere di per sé un illecito, può essere strumentale alla realizzazione di altre fattispecie criminose. I controlli predisposti per prevenire tale fattispecie di reato sono efficaci anche per la prevenzione di altri reati. Tra tali controlli si segnalano:</p> <ul style="list-style-type: none"> <li>• procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro;</li> <li>• modalità di accesso ai sistemi informatici aziendali mediante adeguate procedure di autorizzazione, che prevedano, ad esempio, la concessione dei diritti di accesso ad un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze di accesso derivanti dalle mansioni aziendali che competono al ruolo ricoperto dal soggetto;</li> <li>• procedura per il controllo degli accessi;</li> <li>• tracciabilità degli accessi e delle attività critiche svolte tramite i sistemi informatici aziendali;</li> </ul> |

<sup>2</sup> Va sottolineato come il reato in esame si realizza soltanto se il sistema informatico che si viola sia provvisto di adeguata protezione. La protezione manifesta infatti la volontà del titolare di impedire a terzi l'accesso al sistema e la violazione di essa rende il comportamento illecito

| FATTISPECIE DI REATO   | CASISTICHE   | CONTROLLI PREVENTIVI   |
|--|--|--|
|  | <p>Creazione di utenze non autorizzate e consegna delle corrispondenti credenziali al personale interno all'azienda, in violazione delle procedure di autenticazione e autorizzazione informatica, in modo da rendere possibili accessi abusivi.</p> <p>Emissione dei certificati qualificati per la Firma Digitale e dei certificati per la Carta Nazionale dei servizi (utilizzata per l'accesso ai servizi offerti in rete dalla PA) da parte di un dipendente addetto a tali servizi, sulla base di false dichiarazioni fornite dal richiedente il certificato.</p>  |  |
| <p><b>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche</b><br/>(art. 617-quater c.p.)</p> <p><b>Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche</b><br/>(617-quinquies c.p.)</p> | <p>Intercettazione fraudolenta di comunicazioni di enti concorrenti nella partecipazione a gare di appalto o di fornitura svolte su base elettronica (<i>e-marketplace</i>) per evitare che i concorrenti possano presentare al compratore un'offerta migliore ovvero anche per conoscere l'entità dell'offerta del concorrente stesso, qualora essa non sia in chiaro (tale tipologia di gestione degli acquisti/gare è frequente nell'ambito della PA).</p> <p>Impedimento/interruzione di una comunicazione al fine di evitare che un concorrente trasmetta i dati e/o l'offerta per la partecipazione ad una gara.</p> <p>Intercettazione fraudolenta di una comunicazione tra più parti al fine di veicolare informazioni false o comunque alterate, ad esempio per danneggiare l'immagine di un concorrente.</p> <p>Intercettazione o impedimento di comunicazioni informatiche o telematiche e installazione di apparecchiature atte ad intercettare ed impedire comunicazioni informatiche commessi dal personale incaricato della gestione degli apparati e dei sistemi componenti l'infrastruttura di rete aziendale</p> | <p>Oltre ai controlli generali sopra citati, sono applicati i seguenti controlli:</p> <ul style="list-style-type: none"> <li>• utilizzazione di misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse;</li> <li>• definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi da parte di personale all'uopo incaricato;</li> <li>• previsione di controlli sulla rete aziendale e sulle informazioni che vi transitano;</li> <li>• esistenza di controlli per l'instradamento (<i>routing</i>) della rete, al fine di assicurare che non vengano violate le politiche di sicurezza ;</li> <li>• esistenza di procedure di controllo della installazione di <i>software</i> sui sistemi operativi;</li> <li>• esistenza di procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi.</li> </ul> |

| FATTISPECIE DI REATO   | CASISTICHE   | CONTROLLI PREVENTIVI   |
|--|--|--|
| <p><b>Danneggiamento di informazioni, dati e programmi informatici</b><br/>(art. 635-bis c.p.)</p> <p><b>Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico</b><br/>(art. 615-quinquies c.p.)</p> | <p>Danneggiamento delle infrastrutture tecnologiche dei concorrenti al fine di impedirne l'attività o danneggiarne l'immagine. Con riferimento a tali condotte, sono da considerarsi maggiormente esposti al rischio gli enti la cui attività dipende strettamente dalle infrastrutture tecnologiche, come ad esempio avviene nell'<i>e-commerce</i> o <i>e-banking</i>.</p> <p>Violazione dei sistemi su cui i concorrenti conservano la documentazione relativa ai propri prodotti/progetti allo scopo di distruggere le informazioni e ottenere un vantaggio competitivo.</p> <p>Danneggiamento di informazioni, dati e programmi aziendali causato mediante la diffusione di virus o altri programmi malevoli commessa da soggetti che utilizzano abusivamente la rete o i sistemi di posta elettronica aziendali.</p> <p>Danneggiamento di informazioni, dati, programmi informatici aziendali o di sistemi informatici di terzi, anche concorrenti, commesso dal personale incaricato della loro gestione, nello svolgimento delle attività di manutenzione e aggiornamento di propria competenza.</p> | <p>Oltre ai controlli generali sopra citati, sono applicati i seguenti controlli specifici:</p> <ul style="list-style-type: none"> <li>• formalizzazione di regole al fine di garantire un utilizzo corretto delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;</li> <li>• procedure per l'etichettatura e il trattamento delle informazioni in base allo schema di classificazione adottato dall'ente;</li> <li>• controlli di individuazione, prevenzione e ripristino al fine di proteggere da <i>software</i> dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema;</li> <li>• procedure di controllo della installazione di <i>software</i> sui sistemi operativi;</li> <li>• procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi.</li> </ul> |

| FATTISPECIE DI REATO  | CASISTICHE  | CONTROLLI PREVENTIVI   |
|---|---|--|
| <p><b>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.)</b></p> | <p>Danneggiamento, distruzione o manomissione di documenti informatici aventi efficacia probatoria, registrati presso enti pubblici (es. polizia, uffici giudiziari, ecc.), da parte di dipendenti di enti coinvolti a qualunque titolo in procedimenti o indagini giudiziarie.</p> <p>Danneggiamento di informazioni, dati e programmi informatici utilizzati da enti pubblici commesso dal personale incaricato della gestione dei sistemi di clienti della PA.</p> | <p>Oltre ai controlli generali sopra citati, sono applicati i seguenti controlli specifici:</p> <ul style="list-style-type: none"> <li>• formalizzazione di regole per un utilizzo accettabile delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;</li> <li>• procedure per l'etichettatura ed il trattamento delle informazioni in base allo schema di classificazione adottato dall'organizzazione;</li> <li>• controlli di individuazione, prevenzione e ripristino al fine di proteggere da software dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema;</li> <li>• procedure di controllo della installazione di <i>software</i> sui sistemi operativi;</li> <li>• procedure per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi.</li> </ul> |

| FATTISPECIE DI REATO   | CASISTICHE  | CONTROLLI PREVENTIVI   |
|--|---|--|
| <p><b>Danneggiamento di sistemi informatici o telematici</b><br/>(art. 635-quater c.p.)</p> <p><b>Danneggiamento di sistemi informatici o telematici di pubblica utilità</b><br/>(art. 635-quinquies c.p.)</p> | <p>Danneggiamento di siti <i>web</i> dei concorrenti, sia pubblici che privati, per arrecare loro un danno.</p> | <p>Oltre ai controlli generali sopra citati, sono applicati i seguenti controlli specifici:</p> <ul style="list-style-type: none"> <li>• definizione di regole per un utilizzo accettabile delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;</li> <li>• procedure per l’etichettatura ed il trattamento delle informazioni in base allo schema di classificazione adottato dall’organizzazione;</li> <li>• misure di sicurezza per apparecchiature fuori sede, che prendano in considerazione i rischi derivanti dall’operare al di fuori del perimetro dell’organizzazione;</li> <li>• misure di protezione dell’accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse;</li> <li>• definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi da parte di personale all’uopo incaricato;</li> <li>• presenza di misure per un’adeguata protezione delle apparecchiature incustodite;</li> <li>• previsione di ambienti dedicati per quei sistemi che sono considerati “sensibili” sia per il tipo di dati contenuti sia per il valore di <i>business</i>.</li> </ul> |

| FATTISPECIE DI REATO   | CASISTICHE   | CONTROLLI PREVENTIVI   |
|--|--|--|
| <p><b>Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici</b><br/>(art. 615-quater c.p.)</p> | <p>Detenzione ed utilizzo di <i>password</i> di accesso a siti di enti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate.</p> <p>Detenzione e utilizzo di <i>password</i> per accedere a servizi cui non si avrebbe diritto.</p> <p>Detenzione ed utilizzo di <i>password</i> di accesso alle caselle e-mail dei dipendenti, allo scopo di controllare le attività svolte nell'interesse dell'azienda, anche in violazione di leggi sulla <i>privacy</i> o dello statuto dei lavoratori. Tale condotta non costituisce reato se si accede al computer fornito al dipendente dall'azienda per esigenze indifferibili ed urgenti connesse all'attività operativa.</p> | <p>Oltre ai controlli generali sopra citati sono applicati i seguenti controlli specifici:</p> <ul style="list-style-type: none"> <li>• inclusione negli accordi con terze parti e nei contratti di lavoro di clausole di non divulgazione delle informazioni;</li> <li>• procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro.</li> </ul>                              |
| <p><b>Frode informatica del soggetto che presta servizi di certificazione di firma elettronica</b><br/>(640-quinquies c.p.)</p>  | <p>Rilascio di certificati digitali da parte di un ente certificatore senza che siano soddisfatti gli obblighi previsti dalla legge per il rilascio di certificati qualificati (es. identificabilità univoca del titolare, titolarità certificata, ecc.), con lo scopo di mantenere un elevato numero di certificati attivi.</p> <p>Aggiramento dei vincoli imposti dal sistema usato dall'ente per la verifica dei requisiti necessari al rilascio dei certificati da parte dell'amministratore di sistema allo scopo di concedere un certificato e produrre così un guadagno all'ente.</p>   | <p>Oltre ai controlli generali sopra citati, sono applicati i seguenti controlli specifici:</p> <ul style="list-style-type: none"> <li>• misure volte alla protezione dei documenti elettronici (es. firma digitale);</li> <li>• procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme a disposizioni di legge e contrattuali.</li> </ul> |

## SEZIONE IV

### RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO BENI O UTILITÀ DI PROVENIENZA ILLECITA

#### **Art. 648 del codice penale (Ricettazione)**

Fuori dei casi di concorso nel reato, chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da euro 516 a euro 10.329.

La pena è della reclusione sino a sei anni e della multa sino a euro 516 se il fatto è di particolare tenuità.

Le disposizioni di questo articolo si applicano anche quando l'autore del delitto da cui il denaro o le cose provengono non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto.

#### **Art. 648-bis del codice penale (Riciclaggio)**

Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da Euro 1.032 a Euro 15.493.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. Si applica l'ultimo comma dell'articolo 648.

#### **Art. 648-ter del codice penale (Impiego di denaro, beni o utilità di provenienza illecita)**

Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da euro 1032 a euro 15.493.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

La pena è diminuita nell'ipotesi di cui al secondo comma dell'articolo 648. Si applica l'ultimo comma dell'articolo 648.

**Considerazioni.** Con il D. Lgs. n. 231 del 21 novembre 2007 - in vigore dal 29 dicembre 2007 - 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 criminose e di finanziamento del terrorismo (c.d. III direttiva antiriciclaggio), e alla direttiva 2006/70/CE della Commissione che ne reca misure di esecuzione.

Considerato il tipo di attività svolta da SEWS-Cabind, la tipologia di clienti e fornitori e la loro ricorrenza, si ritiene che il rischio di ricadere in questa fattispecie non sia particolarmente elevato.

**Attività aziendali a rischio.** Le attività aziendali da prendere in considerazione ai fini della prevenzione di tali reati sono principalmente le attività con soggetti terzi, intendendosi per tali quelle relative ai rapporti instaurati tra società e soggetti terzi.

## ATTIVITÀ AZIENDALI A RISCHIO

- Amministrazione (Tesoreria, Personale, ecc.)
- Commerciale
- Finanza
- Direzione acquisiti

**Attività aziendali** a rischio in relazione a:

### **Rapporti con soggetti terzi**

- Contratti di acquisto e/o di vendita con controparti
- Transazioni finanziarie con controparti
- Investimenti con controparti

## CONTROLLI PREVENTIVI SPECIFICI (PROTOCOLLI) E PRINCIPALI ATTIVITÀ DELL'OdV

Verifica dell'attendibilità commerciale e professionale dei fornitori e *partner* commerciali/finanziari, sulla base di alcuni indici rilevanti (es. dati pregiudizievoli pubblici - protesti, procedure concorsuali - o acquisizione di informazioni commerciali sulla azienda, sui soci e sugli amministratori tramite società specializzate; entità del prezzo sproporzionata rispetto ai valori medi di mercato; coinvolgimento di "persone politicamente esposte", come definite all'art. 1 dell'Allegato tecnico del D. Lgs. 21 novembre 2007, n. 231, di attuazione della direttiva 2005/60/CE).

Verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni.

Controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi. Tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie.

## SEZIONE V

### REATI CONTRO LA PERSONALITÀ INDIVIDUALE

L'art. 5 della legge n. 228/2003, in tema di misure contro la tratta delle persone, aggiunge al decreto 231 un articolo 25-quinquies che prevede l'applicazione di sanzioni amministrative alle persone giuridiche, società e associazioni per la commissione di delitti contro la personalità individuale.

L'art. 25-quinquies è stato successivamente integrato ad opera dell'art. 10, legge n. 38 del 6 febbraio 2006, contenente "*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo internet*", che modifica l'ambito di applicazione dei delitti di pornografia minorile e detenzione di materiale pornografico (artt. 600-ter e 600-quater c.p.), includendo anche le ipotesi in cui tali illeciti siano commessi mediante l'utilizzo di materiale pornografico raffigurante immagini virtuali di minori di anni 18 o parti di esse (c.d., pedopornografia virtuale ai sensi del rinvio al nuovo art. 600-quater c.p.).

La citata legge n. 38/2006 è intervenuta anche a modificare le disposizioni di cui agli articoli 600-bis, 600-ter e 600-quater, relativi ai delitti di prostituzione minorile, pornografia minorile e detenzione di materiale pornografico, per i quali era già prevista la responsabilità amministrativa degli enti.

**L'art. 25-quinquies** (*delitti contro la personalità individuale*) stabilisce:

In relazione alla commissione dei delitti previsti dalla sezione I del capo III del titolo XII del libro II del codice penale si applicano all'ente le seguenti sanzioni pecuniarie:

- a) per i delitti di cui agli articoli 600, 601 e 602, la sanzione pecuniaria da quattrocento a mille quote;
- b) per i delitti di cui agli articoli 600-bis, primo comma, 600-ter, primo e secondo comma, anche se relativi al materiale pornografico di cui all'articolo 600-quater 1, e 600-quinquies, la sanzione pecuniaria da duecento a settecento quote;
- c) per i delitti di cui agli articoli 600-bis, secondo comma, 600-ter, terzo e quarto comma, e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater I, la sanzione pecuniaria da duecento a settecento quote.

Nei casi di condanna per uno dei delitti indicati nel comma 1, lettere a) e b), si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a un anno.

Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati nel comma 1, si applica la sanzione dell'interdizione definitiva dell'esercizio dell'attività ai sensi dell'articolo 16, comma 3.

#### **Art. 600 del codice penale** (*riduzione o mantenimento in schiavitù o in servitù*)

Chiunque esercita su una persona poteri corrispondenti a quelli del diritto di proprietà ovvero chiunque riduce o mantiene una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento, è punito con la reclusione da otto a vent'anni.

La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta è attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica

o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona.

La pena è aumentata da un terzo alla metà se i fatti di cui al primo comma sono commessi in danno di minore degli anni diciotto o sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi.

**Considerazioni.** Così come per le altre fattispecie di reato con riguardo alle quali sorge la responsabilità dell'ente, anche i delitti sopra richiamati devono essere commessi nell'interesse o a vantaggio dell'impresa. Pertanto, si è preso in considerazione solo il reato di cui all'art. 600 c.p. poiché per gli altri è praticamente impossibile individuare la sussistenza di un interesse o vantaggio per l'ente (es. prostituzione minorile) in considerazione dell'attività svolta da SEWS-Cabind.

Quando invece ai reati connessi alla schiavitù, oltre a ricordare che tali ipotesi di reato si estendono non solo al soggetto che direttamente realizza la fattispecie illecita, ma anche a chi consapevolmente agevola anche finanziariamente la medesima condotta, è anche qui opportuno prevedere specifiche misure di prevenzione, in quanto è possibile escludere che tali delitti siano commessi in Italia, ma non esistono sufficienti controlli sulle attività delle società estere per escludere totalmente la violazione di norme internazionali in materia.

Si rammenta che, in base all'art. 4 del d.lgs. 231/2001, “gli enti aventi nel territorio dello Stato la sede principale rispondono anche in relazione ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto”.

La certificazione OHSAS 18001 ha ridotto il rischio dell'inottemperanza, da parte delle società controllate in Polonia ed in Marocco, delle normative in materia di diritto del lavoro.

SEWS-Cabind informerà i vertici delle controllate straniere sulle conseguenze che possono scaturire in capo alla società italiana in caso di comportamenti non conformi al nostro ordinamento in materia lavoristica.

## SEZIONE VI

### **“REATI DI OMICIDIO COLPOSO E LESIONI PERSONALI COLPOSE GRAVI O GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO”**

L'art. 25-septies del D.Lgs. 231/2001 si riferisce ai reati di omicidio colposo e lesioni personali colpose gravi e gravissime di cui agli artt. 589 e 590, terzo comma c.p. commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Sul piano dell'elemento soggettivo, l'evento è colposo quando l'agente non vuole la morte o la lesione della vittima, ovvero quando l'evento lesivo si verifica per per negligenza, imperizia o inosservanza di leggi da parte dell'agente stesso. In particolare:

(Art. 589 c.p.) *“Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.*

*Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni.”*

L'omicidio colposo implica la presenza di tre elementi: una condotta, un evento (la morte di una persona) e il nesso di causalità tra l'una e l'altro.

(Art. 590 c.p.) *“Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309.*

*Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619, se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1.239.*

*Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni. Nei casi di violazione delle norme sulla circolazione stradale, se il fatto e' commesso da soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e successive modificazioni, ovvero da soggetto sotto l'effetto di sostanze stupefacenti o psicotrope, la pena per le lesioni gravi e' della reclusione da sei mesi a due anni e la pena per le lesioni gravissime e' della reclusione da un anno e sei mesi a quattro anni.”*

La lesione personale è grave:

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

La lesione personale è gravissima se dal fatto deriva:

- una malattia certamente o probabilmente insanabile;
- la perdita di un senso;
- la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave
- difficoltà dell'uso della parola;
- la deformazione, ovvero lo sfregio permanente del viso.

L'obiettivo della presente SEZIONE VI è la definizione delle regole di condotta da adottarsi da parte di tutti i destinatari (Dipendenti, Organi Sociali, Collaboratori, ecc.), al fine di prevenire il verificarsi dei reati sopra descritti.

SEWS-Cabind adotta e attua efficacemente un idoneo modello organizzativo e di gestione avente efficacia esimente dalla responsabilità amministrativa delle persone giuridiche, delle società e delle assicurazioni anche prive di personalità giuridica di cui al D.Lgs. 231/01, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici, di cui all'art. 30 del D.Lgs. 81/08 (come modificato dal D.Lgs. 106/09), relativi:

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

Il modello organizzativo e gestionale prevede idonei sistemi di registrazione dell'avvenuta effettuazione delle suddette attività e prevede, per quanto richiesto dalla natura e dimensioni di SEWS-Cabind, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il modello organizzativo prevede altresì un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo sono adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

In particolare SEWS-Cabind adotta un Sistema di Gestione della Sicurezza (in seguito SGSL) conforme alla Norma BS OHSAS 18001:2007 che, a norma dell'art. 30 del D.Lgs. 81/08, è ritenuto conforme, per le parti corrispondenti, ai requisiti del Modello organizzativo e gestionale.

Il rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici, è garantito dall'applicazione di:

- 4.3.2 – *“Prescrizioni legali ed altre”*. Questa parte del Manuale del SGSL e la relativa procedura generale di sistema (PGS 4.3 02) stabilisce quali prescrizioni di legge siano vincolanti per SEWS-Cabind e quali altre prescrizioni volontarie l'azienda intende sottoscrivere in materia di salute e sicurezza sul lavoro. Questo strumento permette inoltre di mantenere aggiornate le informazioni sui requisiti legali e volontari al fine di potervi ottemperare nel modo e nei tempi adeguati.
- 4.3.1 – *“Identificazione dei pericoli, valutazione dei rischi loro controllo”*. Attraverso le definizioni contenute nel Manuale del SGSL, le relative procedure generali di sistema (PGS 4.3 01) e le istruzioni di

controllo operativo, si è raggiunto l'obiettivo di valutare tutti i rischi per la salute e la sicurezza durante le attività svolte in SEWS-Cabind e di mantenere sotto controllo il loro livello di rischio.

- 4.4.6 – “*Controllo operativo*”. La definizione delle attività e delle responsabilità connesse al controllo operativo dei processi aziendali, si basa sui risultati della valutazione dei rischi per la salute e la sicurezza. Tiene necessariamente conto di:
  - Tutti i processi e attività pericolose per la salute e la sicurezza dei lavoratori;
  - Acquisto o trasferimento di merci e servizi, uso di risorse esterne;
  - Uso di materiali pericolosi;
  - Eventuali attività di manutenzione di impianti e attrezzature;
  - Eventuale necessità di informazione e formazione.

In modo particolare sono sottoposte ad esame: “*Gestione fornitori Servizi ed Appaltatori*” (PGS 4.4 04), “*La gestione degli agenti chimici*” (PGS 4.4 05), “*Attrezzature di lavoro*” (PGS 4.4 06).

Le attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti sono garantite attraverso:

- 4.3.1 – “*Identificazione dei pericoli, valutazione dei rischi e loro controllo*”. La metodologia aziendale per l'identificazione dei pericoli e la valutazione dei rischi è definita nel rispetto di una logica “preventiva” piuttosto che “correttiva”. SEWS-Cabind nel processo di valutazione dei rischi, tiene conto delle attività, abituali e non, incluse quelle svolte dagli appaltatori e visitatori, e le relative modalità operative, dei dati relativi a infortuni, mancati incidenti, incidenti e malattie professionali. Le azioni da intraprendere per eliminare o ridurre per quanto possibile i rischi, sono stabilite in relazione alla stima di ciascuno di essi (probabilità di accadimento, gravità del danno potenziale, ecc.) e si traducono nella definizione di: procedure di controllo operativo (vedi 4.4.6 del SGSL), esigenze informative e formative del personale (Vedi 4.4.2, 4.4.3 del SGSL), monitoraggio per assicurare l'attuazione e l'efficacia delle misure adottate (vedi 4.5.1 del SGSL).

Le attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza sono regolamentate dalle seguenti parti del Manuale di SGSL:

- 4.4.1 – “*Struttura organizzativa e responsabilità*”. SEWS-Cabind ha definito ruoli e responsabilità aziendali in materia di salute e sicurezza sul lavoro, in relazione ai requisiti legali e volontari applicabili. L'azienda ha identificato e formalizzato, all'interno della propria struttura, una specifica funzione che si occupa del SGSL, associando alla Funzione un Responsabile con l'autorità necessaria e autonomia finanziaria. Il quadro complessivo della struttura gerarchica e organizzativa è schematizzato nell'organigramma aziendale ed evidenzia una struttura basata secondo la logica: Datore di lavoro – Dirigente - Preposto. L'autorità e le responsabilità per l'esecuzione delle attività sono delegate a ciascuno dei Responsabili di Funzione e la gestione corrente del SGSL viene garantita direttamente dai diversi Responsabili, che si avvalgono del supporto del RSPP.
- 4.4.3 – “*Comunicazione, partecipazione e consultazione*”. SEWS-Cabind si impegna a tenere sotto controllo gli aspetti di consultazione, comunicazione e partecipazione, per assicurare chiarezza ed efficacia di comunicazione sia al proprio interno, che verso l'esterno (PGS 4.4 02, PGS 4.4 03). Viene richiesta la partecipazione dei lavoratori, in merito allo sviluppo e revisione della politica, dell'identificazione dei pericoli, alla valutazione dei rischi, alle indagini sugli incidenti, alla definizione e al raggiungimento degli obiettivi del SGSL e alla gestione dei cambiamenti che influiscono sull'ambiente di lavoro.  
In materia di salute e sicurezza, nei modi e nei tempi previsti dalla normativa vigente, SEWS-Cabind consulta preventivamente il Rappresentante dei Lavoratori per la Sicurezza (RLS) in ordine alla valutazione dei rischi, all'individuazione, programmazione, realizzazione e verifica della prevenzione in azienda; sulla

designazione del RSPP, degli addetti alla prevenzione incendi e primo soccorso e del Medico competente; all'organizzazione della formazione.

- 4.4.7 – “*Preparazione e risposta alle emergenze*”. In azienda si sono stabilite e mantenute attive procedure specifiche per individuare le potenziali situazioni di emergenza e le conseguenti risposte di intervento (PGS 4.4 07). Sono state individuati e nominati gli addetti al primo soccorso e all'antincendio, i quali risultano formati e addestrati per il compito specifico ed hanno conoscenza della specifica procedura. L'efficacia degli interventi viene monitorata attraverso periodiche esercitazioni, che simulano situazioni tipiche di emergenza.

Le attività di informazione e formazione dei lavoratori sono assicurate attraverso l'applicazione delle specifiche parti del Manuale SGSL.

- 4.4.2 – “*Competenza, addestramento e consapevolezza*”. L'azienda assicura a tutti i dipendenti un adeguato e specifico livello di istruzione, addestramento o esperienza appropriata in materia di salute e sicurezza sul lavoro.

I fabbisogni formativi richiesti per legge sono mantenuti sotto controllo, in modo da monitorare le scadenze e le necessità di aggiornamento delle figure aziendali preposte alla salute e sicurezza. Inoltre vengono periodicamente valutati i fabbisogni formativi del personale al fine di rendere ciascun lavoratore maggiormente consapevole e responsabile in relazione alle proprie attribuzioni e competenze (PGS 4.4 01). Attraverso un sistema di misurazione e monitoraggio delle prestazioni del SGSL, dai dati statistici di infortuni, mancati incidenti, ecc, dagli esiti delle riunioni periodiche, si ottengono le informazioni necessarie per programmare e attuare piani formativi mirati alla consapevolezza e alla responsabilità di ciascun lavoratore. Lo scopo di queste attività è quello di diffondere sempre di più una cultura aziendale sulla salute e sicurezza sul lavoro, così come stabilito dalla Politica aziendale (vedi 4.2 del SGSL).

Le attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei valti livelli dell'Azienda rientrano nelle specifiche sezioni del Manuale del SGSL che di seguito vengono descritte. All'interno di questa sezione è anche messo sotto controllo il sistema degli obblighi relativi alla sorveglianza sanitaria.

- 4.5.1 – “*Misurazione e monitoraggio dei risultati*”. SEWS-Cabind effettua misure per monitorare, anche a scopo preventivo, la conformità alle prescrizioni legali, il rispetto di quanto pianificato, il raggiungimento degli obiettivi nonché gli aspetti legati alla salute dei lavoratori come l'andamento degli infortuni, incidenti e malattie professionali (PGS 4.5 01). A tale scopo sono definiti nel SGSL degli indicatori di prestazione e delle regole interne di analisi, che evidenziano eventuali non conformità, attivando di conseguenza azioni correttive e preventive proporzionate (vedi 4.5.3 del SGSL). La struttura di analisi prevede la suddivisione delle potenziali non conformità in “Non conformità di sistema” o “Non conformità operative”, in modo da attribuire anche una priorità di intervento.

È stato predisposto uno scadenziario per tenere sotto controllo tutti gli obblighi relativi alla salute e sicurezza, compresa la sorveglianza sanitaria con il supporto del medico competente.

- 4.5.4 – “*Controllo delle registrazioni*”. Sono sottoposte a controllo e registrazione tutte le informazioni connesse alle attività definite nel SGSL. Si tratta di modulistica (di origine interna o esterna) compilata e sottoscritta, di verbali di riunioni, ecc. Attraverso specifici strumenti di identificazione, catalogazione, archiviazione, conservazione, aggiornamento e eliminazione, i documenti di registrazione completano il quadro del monitoraggio delle attività sottoposte a controllo di SGSL o a specifici obblighi di legge (PGS 4.4 03).
- 4.5.5 – “*Audit interni*”. L'azienda pianifica ed esegue periodiche verifiche interne, ovvero esami sistematici ed indipendenti mirati a stabilire se quanto pianificato a livello organizzativo generale o più in dettaglio a livello comportamentale è coerente con quanto stabilito, viene efficacemente attuato, risulta idoneo al conseguimento degli obiettivi e alla politica aziendale. (PGS 4.5 02).

L'acquisizione di documentazioni e certificazioni obbligatorie di legge sono garantite attraverso l'applicazione delle seguenti sezioni del Manuale del SGSL:

- 4.4.4 – “*Documentazione*”. L'insieme delle indicazioni contenute in tutti i documenti del SGSL, oltre a contribuire all'effettiva realizzazione delle attività pianificate, è un forte strumento di circolazione delle informazioni generali e consente a tutti di avere un quadro costantemente ordinato ed aggiornato in materia di salute e sicurezza sul lavoro, in relazione alle proprie attribuzioni e competenze.
- 4.4.5 – “*Controllo dei documenti e dei dati*”. In modo particolare in azienda si è organizzato un sistema di identificazione della documentazione (origine interna o esterna, ecc.) in modo da gestire le informazioni in esse contenute e attivare le figure aziendali o gli enti interessati al fine di ottenere il risultato atteso (certificazioni, ecc.) (PGS 4.4 03).
- 4.5.4 – “*Controllo delle registrazioni*”. Sono sottoposti a registrazione tutti i documenti e le certificazioni inerenti la salute e la sicurezza. Le modalità operative di gestione delle registrazioni sono definite nella procedura PGS 4.5 04. Nello specifico la documentazione inerente gli aspetti legislativi, prescrittivi, autorizzativi è conservata senza limiti temporali, così come la documentazione inerente l'evidenza delle misure finalizzate alla sicurezza dei lavoratori. Gli atti documentali inerenti il SGSL sono invece conservati per tempo variabili a seconda del tipo di documento (vedi registri della procedura PGS 4.5 04).

SEWS-Cabind programma ed effettua periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate, attraverso la definizione e l'applicazione delle seguenti sezioni del Manuale del SGSL:

- 4.5.5 – “*Audit interni*”.
- 4.6 – “*Riesame della direzione*”. SEWS-Cabind gestisce ed attua il riesame del SGSL, con periodicità annuale (o scadenza più ravvicinata qualora ne emerga la necessità o siano evidenziati significativi cambiamenti nell'organizzazione o nel quadro di riferimento esterno). Il riesame da evidenza di un approccio al miglioramento continuo delle prestazioni in materia di salute e sicurezza e alla prevenzione di incidenti e infortuni.

SEWS-Cabind ha, inoltre, ritenuto opportuno richiedere la certificazione di parte terza relativamente al sistema di gestione della sicurezza realizzato secondo lo schema BS OHSAS 18001 e mantiene attiva tale certificazione sottoponendo il sistema alle visite di sorveglianza e rinnovo da parte dell'Organismo di certificazione accreditato, previste dallo schema di accreditamento del SINCERT.

Come previsto dal comma 4 dell'art. 30 del D.Lgs. 81/08 il modello organizzativo di SEWS-Cabind prevede un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il modello organizzativo utilizza le informazioni e i risultati del Sistema di Gestione per la Salute e Sicurezza sul lavoro come elemento di discussione in fase di riesame del modello organizzativo, da cui può nascere un'eventuale esigenza di modifica del modello stesso. In modo particolare saranno presi in considerazione situazioni che comportino violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene del lavoro che conducano ai reati di omicidio colposo e lesioni gravi e gravissime di cui agli artt. 589 e 590, terzo comma c.p.

Collegno, 25 novembre 2009

**L'AMMINISTRATORE DELEGATO**



Hiroshi Sotome