_Italia

AXIANS ITALIA S.P.A.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS 231/01

PARTI SPECIALI

axians

Sommario

0. Premessa 5

Parte speciale 1 6

Reati contro la Pubblica Amministrazione 6

1. I reati contro la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/01) 6

1.1. Fattispecie di reato 6

1.2. Definizione di Pubblica Amministrazione, Pubblico Ufficiale e Incaricato di pubblico servizio 7

2. Attività sensibili 8

3. Principi generali di comportamento 9

4. Protocolli specifici di comportamento 10

5. Reporting all'Organismo di Vigilanza 19

Parte speciale 2 21

Omicidio colposo e lesioni personali colpose commessi con violazione delle norme antinfortunistiche e di tutela dell'igiene e della salute sul lavoro 21

1. I reati in materia di salute e sicurezza sui luoghi di lavoro (art. 25-septies del D.Lgs. 231/01) 21

2. Attività sensibili 21

3. Principi generali di comportamento 24

4. Protocolli specifici di comportamento 25

5. Reporting all'Organismo di Vigilanza 29

Parte Speciale 3 30

Reati Societari 30

1. I reati societari (art. 25-ter del D.Lgs. 231/2001) 30

2. Attività sensibili 30

3. Principi generali di comportamento 31

4. Protocolli specifici di comportamento 31

5. Reporting all'Organismo di Vigilanza 33

Parte Speciale 4 35

Delitti informatici e trattamento illecito di dati e violazione del diritto d'autore 35

1. I reati informatici, trattamento illecito di dati e violazione del diritto d'autore (artt. 24-bis e 25-novies del D.Lgs. 231/2001) 35

2. Attività sensibili 37

3. Principi generali di comportamento 37
4. Protocolli specifici di comportamento 39
5. Reporting all'Organismo di Vigilanza 43
Parte Speciale 5 44
Corruzione tra privati 44
1. I delitti di corruzione tra privati e istigazione alla corruzione tra privati 44
2. Attività sensibili 44
3. Principi generali di comportamento 45
4. Protocolli specifici di comportamento 45
5. Reporting all'Organismo di Vigilanza 47
Parte Speciale 6 46
Delitti di criminalità organizzata, transnazionali e di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria 48
1. Reati di criminalità organizzata, reati transnazionali e delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (artt. 24-ter, 25-decies del D. Lgs. 231/2001 e art. 10 della L. 146/2006) 48
2. Attività sensibili 49
3. Principi generali di comportamento 50
4. Protocolli specifici di comportamento 50
5. Reporting all'Organismo di Vigilanza 52
Parte Speciale 7 53
Reati contro l'industria e il commercio e in materia di falsità 53
1. Le fattispecie contro l'industria e il commercio e in materia di falsità in monete, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento (artt. 25-bis.1 e 25-bis del D. Lgs. 231/2001) 53
2. Attività sensibili 53
3. Principi generali di comportamento 54
4. Protocolli specifici di comportamento 54
5. Reporting all'Organismo di Vigilanza 56
Parte Speciale 8 57
Reati di ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita 57
1. Le fattispecie di riciclaggio, autoriciclaggio, reimpiego (art. 25-octies del D. Lgs. 231/2001) 57
2. Attività sensibili 57
3. Principi generali di comportamento 57

4. Protocolli specifici di comportamento 58
5. Reporting all'Organismo di Vigilanza 59
Parte Speciale 9 60
Reati ambientali 60
1. I reati ambientali (art. 25-undecies del D. Lgs. 231/2001) 60
2. Attività sensibili 61
3. Principi generali di comportamento 62
4. Protocolli specifici di comportamento 63
5. Reporting all'Organismo di Vigilanza 64
Parte Speciale 10 65
Reati tributari 65
1. I reati tributari (art. 25-quinquesdecies del D. Lgs. 231/2001) 65
2. Attività sensibili 65
3. Principi generali di comportamento 66
4. Protocolli specifici di comportamento 67
5. Reporting all'Organismo di Vigilanza 74
Parte Speciale 11 75
Contrabbando e violazioni restrittive dell'Unione Europea 75
1. Le fattispecie in materia di contrabbando (art. 25-sexiesdecies del D. Lgs. 231/2001) 75
2. Le fattispecie in materia di violazioni delle misure restrittive dell'unione europea (art. 25-octies.2 del d. lgs. 231/2001) 77
3. Attività sensibili 78
4. Principi generali di comportamento 78
5. Protocolli specifici di comportamento 79
6. Reporting all'Organismo di Vigilanza 83

0. Premessa

La presente Parte Speciale è stata elaborata tenendo conto dei risultati della valutazione del rischio (c.d. "*risk self-assessment*" o "mappatura"), con la quale AXIANS ha provveduto all'identificazione delle aree di attività in cui possono, in astratto, essere commessi i reati previsti dal Decreto. La mappatura è stata condotta valutando il contesto aziendale in cui la Società opera, attraverso interviste ai soggetti aziendali di ciascuna Funzione/Direzione competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore di attività.

Al fine di prevenire o mitigare il rischio di commissione dei reati-presupposto, AXIANS ha pertanto rappresentato nelle singole Sezioni della presente Parte Speciale, in relazione ad ogni famiglia di reato ritenuta applicabile e rilevante per la Società:

- le attività aziendali sensibili;
- principi di comportamento di carattere generale che devono essere osservati al fine di prevenire il rischio di commissione del reato;
- protocolli specifici di comportamento a presidio di ciascun reato.

Sono inoltre stati declinati i protocolli generali di controllo validi e applicabili a tutti i processi strumentali/funzionali individuati nella realtà organizzativa della Società, indipendentemente dallo specifico rischio reato (par. 8 della Parte Generale).
La definizione dei protocolli specifici di comportamento per ciascun processo sensibile garantisce il rispetto dei protocolli di controllo generali.

axians

Parte speciale 1

Reati contro la Pubblica Amministrazione

La presente Parte Speciale si riferisce ai reati realizzabili nell'ambito dei rapporti tra la società e la Pubblica Amministrazione, come dettagliatamente definiti nell'**Allegato A**. Parte della clientela di AXIANS è costituita da Pubbliche Amministrazioni, in favore delle quali la Società eroga parte dei propri servizi, partecipando - autonomamente, in qualità di appaltatore o sub-appaltatore, ovvero attraverso raggruppamenti temporanei di imprese (R.T.I.) - a gare pubbliche. La Società intrattiene altresì rapporti con la Pubblica Amministrazione, ad esempio, in occasione della presentazione di richieste per l'ottenimento di provvedimenti amministrativi (autorizzazioni, licenze, ecc.) o erogazioni pubbliche (finanziamenti, contributi, ecc.) o nel caso in cui sia sottoposta a visite e/o ispezioni da parte delle Autorità.

1. I reati contro la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/01)

1.1 Fattispecie di reato

In considerazione della mappatura dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati:

- malversazione a danno dello Stato (art. 316-bis c.p.);
- indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.);
- turbata libertà degli incanti (353 c.p.);
- turbata libertà del procedimento di scelta del contraente (353-bis c.p.);
- truffa in danno dello Stato o di altro Ente Pubblico (art. 640, comma 2 n. 1, c.p.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640-ter c.p.);
- peculato (art. 314 comma 1 c.p.);
- indebita destinazione di denaro o cose mobile
- (art. 314-bis c.p.);
- peculato mediante profitto dell'errore altrui (art. 316 c.p.);
- corruzione per l'esercizio della funzione (art. 318 c.p.);
- corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
- corruzione in atti giudiziari (art. 319-ter c.p.);
- induzione indebita a dare o promettere utilità (art. 319-quater c.p.);

- corruzione di persona incaricata di pubblico servizio (art. 320 c.p.);istigazione alla corruzione (art. 322 c.p.);
- Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di

organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.);
- traffico illecito di influenze (art. 346-bis c.p.);
- frode nelle pubbliche forniture (art. 356 c.p.).

Per una disamina approfondita dei reati sopra elencati e delle sanzioni applicabili all'ente si rimanda all'**Allegato A**.

1.2 Definizione di Pubblica Amministrazione, Pubblico Ufficiale e Incaricato di pubblico servizio

Per Pubblica Amministrazione (di seguito "**PA**") si intende, in estrema sintesi, l'insieme dei soggetti – pubblici o privati – che esercitano una funzione pubblica o un pubblico servizio.

Per funzione pubblica si intendono le attività disciplinate da norme di diritto pubblico che attengono alle funzioni legislativa (Stato, Regioni, Province autonome, Comuni, ecc.), amministrativa (membri delle amministrazioni statali e territoriali, Forze dell'Ordine, membri delle amministrazioni sovranazionali, membri delle Authority, delle camere di commercio, membri di commissioni edilizie, collaudatori di opere pubbliche, ecc.), giudiziaria (Giudici, Ufficiali Giudiziari, organi ausiliari dell'Autorità Giudiziaria quali curatori fallimentari o liquidatori, etc.).

La funzione pubblica è caratterizzata dall'esercizio di:

(i) poteri autoritativi, cioè quei poteri che permettono alla Pubblica Amministrazione di realizzare i propri fini mediante veri e propri comandi, rispetto ai quali il privato si trova in una posizione di soggezione. Si tratta dell'attività in cui si esprime il cosiddetto potere d'imperio, che comprende sia il potere di coercizione (arresto, perquisizione, ecc.) e di contestazione di violazioni di legge (accertamento di contravvenzioni, ecc.), sia i poteri di supremazia gerarchica all'interno di pubblici uffici;

(ii) poteri certificativi, che attribuisce ai certificatori il potere di attestare un fatto con efficacia probatoria.

Per pubblico servizio si intendono, invece, le attività disciplinate da norme di diritto pubblico e quelle attività caratterizzate dalla mancanza dei poteri autoritativi o certificativi tipici della funzione pubblica, con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale.

I soggetti che rappresentano la Pubblica Amministrazione o che svolgono una funzione pubblica o un pubblico servizio e con cui è instaurato un rapporto diretto, sono denominati "Pubblici Ufficiali" o "Incaricati di pubblico servizio".

In particolare, per Pubblico Ufficiale si intende, agli effetti della legge penale, il soggetto che esercita "*una pubblica funzione legislativa, giudiziaria o amministrativa*" (art. 357 c.p.).

La norma chiarisce solo la nozione di "*pubblica funzione amministrativa*" (poiché le altre due non hanno suscitato dubbi interpretativi) precisando che, agli effetti della legge penale "*è pubblica la funzione*

amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".

In altre parole, è definita pubblica la funzione amministrativa disciplinata da "*norme di diritto pubblico*", ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

A titolo esemplificativo e non esaustivo, si considerano Pubblici Ufficiali i membri delle amministrazioni statali e territoriali, i membri delle amministrazioni sovranazionali (ad esempio dell'Unione Europea), i membri delle Autorità di Vigilanza, i NAS, i membri delle Forze dell'Ordine e della Guardia di Finanza, i membri delle camere di commercio, gli amministratori di enti pubblici economici, i membri delle commissioni edilizie, i giudici, gli ufficiali giudiziari, gli organi ausiliari dell'Autorità Giudiziaria (ad esempio, i curatori fallimentari).

Al contrario, sono considerati Incaricati di Pubblico Servizio i soggetti "*i quali, a qualunque titolo, prestano un pubblico servizio*" (art. 358 c.p.). Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale.

Ad esempio, possono essere considerati Incaricati di pubblico servizio i dipendenti dell'INAIL, dell'INPS, i dipendenti di aziende energetiche municipali, di uffici postali, uffici doganali, i membri dei consigli comunali, i dipendenti del SSN, gli addetti all'ufficio cassa di un ente pubblico, i dipendenti di enti ospedalieri, delle ASL.

2. Attività sensibili

I reati previsti dagli artt. 24 e 25 del D.Lgs. 231/2001 sono configurabili nell'ambito dei rapporti, sia in Italia sia all'estero, con la Pubblica Amministrazione e con tutti quei soggetti che possono essere qualificati pubblici ufficiali o incaricati di pubblico servizio. Con riferimento a tali reati, i processi sensibili ritenuti maggiormente a rischio in relazione all'attività aziendale di AXIANS, sono i seguenti:

A. gestione dei rapporti con la Pubblica Amministrazione, quali a titolo esemplificativo:

1) partecipazione a procedure ad evidenza pubblica;

2) presentazione di richieste per l'ottenimento di provvedimenti amministrativi (es. autorizzazioni, licenze, permessi ecc.);
3) richiesta e l'ottenimento di contributi, finanziamenti, mutui agevolati e altre erogazioni pubbliche;
4) gestione delle ispezioni (amministrative, fiscali, previdenziali, in materia antinfortunistica ecc.);
5) gestione del contenzioso;

B. gestione di *software* di soggetti pubblici e degli accessi a sistemi informativi della PA;
C. approvvigionamento di beni e servizi e assegnazione di incarichi di consulenza;
D. gestione dei rapporti con agenti e intermediari;
E. gestione di incassi e pagamenti e tesoreria;
F. gestione dei rimborsi spese a dipendenti e collaboratori comprese eventuali spese di rappresentanza;
G. gestione delle sponsorizzazioni e concessione di donazioni, omaggi e liberalità;
H. selezione, assunzione e gestione del personale.

3. Principi generali di comportamento

Le disposizioni della presente Parte Speciale si applicano a tutti i Destinatari del presente Modello che, a qualunque titolo e per conto o nell'interesse di AXIANS, intrattengano rapporti con la Pubblica Amministrazione, ivi compresi i consulenti, i fornitori e i partner commerciali della Società, in forza di apposite clausole contrattuali.

In particolare, coerentemente con i principi deontologici aziendali di cui al presente Modello e con i Codici di Gruppo, è fatto espresso divieto ai Destinatari di:

a) porre in essere, concorrere o dare causa a comportamenti che, presi individualmente o collettivamente, possano configurare, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del D.Lgs. 231/2001);
b) effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri;
c) promettere o versare somme o beni in natura a qualsiasi soggetto (sia esso un dirigente, funzionario o dipendente della Pubblica Amministrazione o un soggetto privato) per promuovere o favorire gli interessi della Società anche a seguito di illecite pressioni. Sono consentiti omaggi e cortesie di uso commerciale di modesto valore, secondo quanto previsto dalla procedura "*PMOG03 Gestione Omaggi & Inviti*";
d) ricorrere a forme diverse di aiuti o contribuzioni, anche sottoforma di sponsorizzazioni, incarichi, consulenze o pubblicità, che abbiano invece le stesse finalità sopra vietate;
e) accordare vantaggi di qualsiasi natura (ad es. promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione italiana o straniera che possano determinare le stesse conseguenze previste al precedente punto b);
f) selezionare personale ovvero favorire l'avanzamento interno di carriera o il riconoscimento di premi per il raggiungimento di obiettivi a beneficio di taluni dipendenti, non ispirandosi a criteri strettamente meritocratici o in base a criteri di valutazione non oggettivi;
g) assumere personale gradito a pubblici ufficiali, a meno che la selezione non abbia seguito un processo ispirato reali esigenze aziendali, a criteri di valutazione oggettivi, e rigorosamente meritocratici;
h) effettuare prestazioni in favore dei consulenti e dei partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
i) assegnare incarichi di fornitura a persone o società vicine o gradite a soggetti pubblici in assenza dei necessari requisiti di qualità, sicurezza e convenienza dell'operazione di acquisto;
j) creare fondi a fronte di beni/servizi contrattualizzati a prezzi superiori a quelli di mercato oppure di fatturazioni inesistenti in tutto o in parte;

k) assegnare incarichi o negoziare condizioni contrattuali con controparti vicine / gradite a soggetti pubblici o legate a dipendenti o collaboratori della Società da interessi personali, in assenza di riconosciuti requisiti di qualità e convenienza economica dell'operazione
l) riconoscere compensi in favore di consulenti, agenti o intermediari che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
m) presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
n) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;
o) violare i sistemi informatici della Pubblica Amministrazione al fine di ottenere informazioni o manipolare le informazioni a vantaggio della Società.

4. Protocolli specifici di comportamento

Ad integrazione delle norme di comportamento di cui sopra ed al fine di fornire un dettaglio operativo rispetto ai principi già declinati nel Codice Etico, nel Codice di Condotta Anticorruzione e nelle *policy* di Gruppo, la Società ha formalizzato le specifiche procedure e protocolli aziendali aventi ad oggetto i processi a rischio identificati:

- PMOG04_Procedura Rapporti con la PA;
- PRO01_Bidding Procedure;
- PMOG03_Gestione Omaggi e Inviti;
- VEI_ Guidelines Omaggi e Inviti BU_Level;
- PURU01_Gestione della ricerca e della selezione del personale;
- PURU03_Gestione e sviluppo delle risorse umane;
- PMOG05_Procedura Gestione Flussi Finanziari ed Economici;
- PDSG11_Gestione Trasferte Estero;
- PURU10_Travel Policy;
- PRO15_Qualificazione e valutazione fornitori;
- PRO13_Gestione degli Acquisti;
- PRO16_Gestione dei rapporti consulenziali.

In aggiunta a tali presidi di controllo, si prevedono i seguenti ulteriori protocolli specifici di comportamento:

A. Gestione dei rapporti con la Pubblica Amministrazione

In base alla Procedura "*PMOG04 Procedura Rapporti con la PA*", ai Codici e alle *policy* di Gruppo:

- i rapporti con la PA e con i soggetti alla stessa riconducibili possono essere tenuti esclusivamente dai soggetti all'uopo autorizzati in base al sistema di deleghe interne e procure in vigore;
- deve essere garantita la tracciabilità delle relazioni con esponenti della PA, attraverso la compilazione di apposito report;
- ogni comunicazione con la Pubblica Amministrazione deve essere effettuata per iscritto, tramite gli appositi canali ufficiali (portale dell'ente pubblico o PEC);
- ogni accordo con la PA o con esponenti della stessa deve essere documentato;
- è espressamente vietato promettere o versare somme di denaro, promettere o concedere beni in natura o altri benefici a enti esponenti/rappresentanti della P.A., ovvero altre organizzazioni con la finalità di promuovere o favorire interessi della Società, anche a seguito di illecite pressioni; oppure promettere o dare seguito a richieste di assunzione in favore di rappresentanti/esponenti della P.A. ovvero di soggetti da questi indicati, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare qualsiasi vantaggio alla Società;
- eventuali criticità o conflitti d'interesse emersi nell'ambito dei rapporti con la PA devono essere prontamente segnalati all'Organismo di Vigilanza;
- nessun Destinatario può da solo e liberamente accedere alle risorse finanziarie e/o effettuare operazioni finanziarie senza attività di controllo e verifica di un'altra funzione aziendale; a tal fine, sono individuati i soggetti autorizzati ad accedere alle risorse finanziarie della Società;
- è fatto divieto di proporre opportunità commerciali che possano avvantaggiare dipendenti della PA a titolo personale o accordare altri vantaggi di qualsiasi natura (es. assunzione del personale) in favore di rappresentanti della PA o di soggetti collegati.

A.1 Partecipazione a procedure di evidenza pubblica

La Società ha ottenuto la certificazione SOA per la partecipazione a gare pubbliche. In base alle *policy* di Gruppo e alle procedure aziendali:

- sussiste una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e, quindi, tra chi predispone e chi sottoscrive la documentazione da presentare alla PA;
- sono chiaramente individuati i soggetti autorizzati alla presentazione delle offerte alla PA; a tal fine, la Procedura "*PRO01 Bidding Procedure*" prevede diversi livelli autorizzativi dell'opportunità commerciale in funzione del valore della stessa e dell'Area di competenza;
- la documentazione di gara deve essere presentata in modalità telematica, previa verifica del possesso dei requisiti prescritti nel bando e controllo della regolarità della stessa, coinvolgendo, ove necessario, il *Legal Counsel*;
- la documentazione di cui sopra è sottoscritta dall'Amministratore Delegato e/o dal *BU Manager* munito di apposita procura;
- conservato un registro delle gare partecipate durante l'anno (*file Excel* in cui sono riportate le informazioni più rilevanti rispetto alla gara, quali, a titolo esemplificativo: tipologia di gara, ente,

vendor, base d'asta, offerta presentata dalla Società, ribasso, esito della gara);
- è garantita la corretta conservazione di tutta la documentazione di gara tramite apposito archivio informatico accessibile soltanto al personale autorizzato;
- è compiutamente rendicontato ("*Nota informativa*") l'utilizzo di eventuali contributi, finanziamenti, mutui o somme comunque denominate, concesse alla Società ed erogate dallo Stato, da altri enti pubblici o dall'Unione Europea;
- è espressamente vietato qualsiasi comportamento volto a influenzare - direttamente o indirettamente - le decisioni della Pubblica Amministrazione;
- è espressamente vietato minacciare i partecipanti a gare di arrecare loro un danno ingiusto o promettere indebiti vantaggi al fine di dissuaderli dalla partecipazione o per conoscere le loro offerte e formulare le proprie in modo tale da ottenere l'aggiudicazione della gara;
- è fatto divieto porre in essere artifici o raggiri tali da indurre in errore la PA a valutare in modo errato le caratteristiche dei prodotti o servizi offerti o forniti;
- ogni anomalia riscontrata deve essere tempestivamente segnalata all'OdV

In particolare: turbata libertà degli incanti e turbata libertà del procedimento di scelta del contraente

La Legge 9 ottobre 2023, n. 137 ha modificato l'art. 24 D. Lgs. 231/2001 introducendo nel catalogo dei reati presupposto anche le fattispecie di cui all'art. 353 c.p. (turbata libertà degli incanti) e art. 353-bis c.p. (turbata libertà del procedimento di scelta del contraente). Si tratta di reati previsti dal Legislatore al fine di tutelare da un lato il buon andamento della P.A., sotto il profilo della garanzia di una libera concorrenza nelle gare organizzate dagli enti pubblici, dall'altro la libertà dei soggetti privati a partecipare alle procedure di cui la norma fa menzione (c.d. diritto individuale all'uguaglianza competitiva).

Per "incanto" si deve intendere tutto ciò che mette in competizione i contraenti purchè si tratti di una gara nei pubblici incanti o nelle licitazioni private per conto della P.A. o per conto di privati. Pertanto, è sufficiente una procedura di gara anche informale e atipica purché condotta in ordine ad una reale e libera competizione tra i soggetti che vi partecipano. Anche il concetto di "turbamento" si deve considerare ampio, potendo essere inteso come l'alterazione, il disturbo, il condizionamento della gara o del procedimento di scelta del contraente, lo sviamento del suo normale *iter* in ragione della finalità di inquinamento del futuro contenuto del bando, di un atto a questo equipollente o della scelta del contraente.
- A seguito del *risk assessment* effettuato e alla luce dell'attività commerciale della Società, che comprende la partecipazione a incanti, al fine di prevenire tali reati si richiamano i principi di comportamento sopra elencati. È fatto divieto ai Destinatari di blandire i pubblici ufficiali, gli incaricati di pubblico servizio, gli altri potenziali contraenti e/o qualsiasi altro soggetto a vario titolo coinvolto nel processo decisionale al fine di influenzarne l'esito. Si devono intendere quali "blandizie", a titolo esemplificativo: omaggi, promesse, liberalità, attività di beneficenza a favore dell'ente pubblico, sostegno alla formazione/ricerca anche mediante borse di studio, utilità;
- offrire regalie ai pubblici ufficiali, agli incaricati di pubblico servizio, agli altri potenziali contraenti e/o a qualsiasi altro soggetto a vario titolo coinvolto nel processo decisionale di propria iniziativa, attingendo a fondi personali o sociali di propria iniziativa e senza specifica autorizzazione dell'Organo amministrativo, al di fuori delle somme annualmente stanziate;
- porre in essere accordi fraudolenti con altri potenziali contraenti attraverso offerte "di comodo" o

"di cortesia" (es. mancata presentazione delle offerte, rotazione delle offerte o spartizione del mercato);

- avere contatti con la P.A. in violazione del Codice Etico e del Codice Anticorruzione;
- alterare in qualsiasi modo il regolare svolgimento dei processi decisionali della PA.

A.2 Presentazione di istanze per il rilasco di provvedimenti amministrativi e richiesta e ottenimento di finanziamenti, contributi, mutui agevolati e altre forme analoghe di erogazioni pubbliche

In aggiunta ai protocolli di cui sopra, in relazione alla presentazione di istanze per l'ottenimento di provvedimenti amministrativi (autorizzazioni, licenze, permessi ecc.) ovvero di contributi, finanziamenti, mutui agevolati e altre erogazioni analoghe, la Procedura "*PMOG04 Gestione rapporti con la PA*" prevede che:

- la richiesta può essere presentata soltanto dai soggetti autorizzati, previa autorizzazione di un Amministratore dotato dei necessari poteri;
- il soggetto incaricato di predisporre la richiesta è tenuto a riportare in modo esatto le informazioni ricevute dalle funzioni aziendali coinvolte; ciascuna funzione è responsabile della veridicità e completezza delle informazioni trasmesse;
- deve essere garantita la tracciabilità delle richieste presentate alla PA mediante compilazione di apposito report contenente gli estremi della richiesta, la relativa data di presentazione, nonché il nominativo e la sottoscrizione della persona fisica responsabile della richiesta stessa;
- la documentazione relativa all'istanza deve essere conservata e archiviata a cura della funzione che effettua la richiesta;
- la documentazione attestante il permanere delle condizioni e dei presupposti indicati dalla normativa che legittimano l'erogazione deve essere diligentemente conservata, così come il rendiconto dell'impiego delle somme concesse;
- in caso di anomalie, l'iter di presentazione della richiesta deve essere sospeso e la problematica andrà segnalata senza indugio all'OdV;
- è fatto divieto di distrarre, anche solo parzialmente, i contributi, le sovvenzioni ed i finanziamenti pubblici dalle finalità per le quali sono stati ottenuti;
- in caso di ottenimento di erogazioni, contributi o finanziamenti da parte di enti pubblici, deve essere predisposto un apposito rendiconto sull'effettiva utilizzazione dei fondi ottenuti ("*Nota informativa*"); tutta la documentazione deve essere archiviata in apposite cartelle accessibili solo al personale autorizzato.

A.3 Gestione degli adempimenti in occasione di visite/ispezioni da parte della PA

In base a quanto previsto dalla Procedura "*PMOG04 Procedura Rapporti con la PA*", in caso di visite o ispezioni da parte degli Organi di Controllo (es. ASL, VV.FF., ARPA, etc.):

- è necessario che alle ispezioni/visite partecipino almeno due soggetti muniti di apposita delega;
- è fatto obbligo garantire la massima cooperazione nei confronti dei Pubblici Ufficiali in caso di visite/ispezioni;
- è fatto divieto nascondere, alterare, falsificare o distruggere documenti in violazione della politica di conservazione dei documenti di AXIANS ovvero dei documenti che possono formare oggetto di

richiesta da parte dei Pubblici Funzionari nell'ambito di una ispezione preannunziata o in corso di esecuzione, ovvero in conseguenza di un ordine legittimo dei Pubblici Funzionari;
- è fatto divieto di tenere una condotta ingannevole, che possa indurre i Pubblici Funzionari in errore di valutazione della documentazione presentata per gli adempimenti necessari;
- è fatto divieto omettere informazioni dovute o fornire informazioni non veritiere al fine di orientare a proprio favore le decisioni degli esponenti della PA procedenti;
- al termine della visita/ispezione le funzioni che vi hanno preso parte predispongono un report interno da allegare al verbale rilasciato dall'Autorità procedente;
- la documentazione relativa alla visita/ispezione è archiviata a cura delle funzioni che hanno preso parte all'ispezione.

A.4 Gestione del contenzioso

Oltre a quanto stabilito dalla Procedura "*PMOG04 Procedura Rapporti con la PA*", in relazione alla gestione del contenzioso, giudiziale e stragiudiziale, si applicano ai Destinatari i seguenti protocolli di comportamento:

- la rappresentanza della Società dinanzi all'Autorità Giudiziaria e la sottoscrizione di accordi transattivi è riservata ai soggetti muniti di apposita procura;

- è fatto divieto di elargire, promettere o dare denaro o altra utilità a giudici, arbitri, funzionari di cancelleria, periti, testimoni ecc., ovvero a persone comunque indicate da codesti soggetti, nonché adottare comportamenti – anche a mezzo di soggetti terzi – contrari alla legge e ai presidi aziendali, per influenzare indebitamente le decisioni dell'organo giudicante ovvero le posizioni della Pubblica Amministrazione, quando questa sia una parte nel contenzioso; eventuali contenziosi/contestazioni o altre problematiche che possano avere rilevanza ai sensi del Decreto devono essere comunque portati a conoscenza del Consiglio di Amministrazione e dell'OdV;
- deve essere verificata con cadenza periodica la situazione dei crediti aziendali, con particolare riguardo ai crediti scaduti;
- eventuali accordi transattivi devono essere definiti attraverso i) l'analisi dell'evento da cui deriva la controversia e dell'esistenza dei presupposti per addivenire alla transazione, ii) la gestione delle trattative finalizzate alla definizione e alla formalizzazione della transazione, iii) la redazione di stipula ed esecuzione dell'accordo transattivo;
- ogni transazione con la PA deve essere verificabile *ex post* tramite adeguati supporti documentali.

B. Gestione di *software* di soggetti pubblici e accesso a sistemi informativi della PA

In relazione a tali attività a rischio-reato, tutti i Destinatari sono tenuti a:

- adottare i protocolli di sicurezza informatica e quelli eventualmente indicati dalla PA;
- garantire l'autenticazione individuale del soggetto operante sul *software*;
- astenersi dal violare i sistemi informativi della PA al fine di ottenere o manipolare informazioni a vantaggio della Società.

C. Approvvigionamento di beni e servizi, assegnazione di incarichi di consulenza e fornitori

Oltre a quanto specificamente previsto dalle procedure "*PRO15 Qualificazione e valutazione fornitori*" e "*PRO13 Gestione degli Acquisti*", la Società assicura che:

- i fornitori, consulenti e gli appaltatori siano scelti in modo trasparente, previa verifica dell'affidabilità e dell'onorabilità degli stessi (ad esempio, verificandone l'iscrizione in Camera di Commercio, la regolarità contributiva con acquisizione di DURC/DURF, ecc.); a tal fine, la Società ha istituito un elenco di fornitori qualificati (*file Excel* disponibile sul *server* aziendale che indica, per ciascun fornitore, la tipologia di servizi forniti, le modalità con cui l'erogazione è regolata, il numero e l'importo degli ordini, il *rating* assegnato, ecc.), la cui compilazione e aggiornamento è di competenza dell'Ufficio Acquisti;
- la scelta dei fornitori, consulenti, appaltatori sia effettuata dopo avere esaminato e valutato più offerte, nei casi previsti dalle procedure aziendali e salvo deroghe disposte in conformità alle stesse o legate alla natura ed alle esigenze dello specifico incarico;
- in conformità alle *policy* di Gruppo, i dieci principali fornitori, subappaltatori e clienti siano sottoposti periodicamente a verifiche reputazionali (c.d. "*business partner screening*");
- gli accordi con terze parti e, in particolare, con fornitori, consulenti, appaltatori, agenti e partner siano definiti per iscritto, con l'evidenziazione di tutte le condizioni e i termini dell'accordo. In virtù di tali accordi, la controparte si impegna al rispetto delle previsioni di cui al D. Lgs. 231/2001, del Modello Organizzativo di AXIANS e dei Codici di Gruppo (c.d. "*clausole 231*");
- gli accordi di cui al precedente punto siano sottoscritti da persone munite dei necessari poteri, in conformità al sistema di deleghe e procure vigente;
- è fatto divieto di riconoscere compensi o effettuare prestazioni in favore di fornitori, consulenti, appaltatori e terze parti in genere che non trovino adeguata giustificazione in relazione al tipo di incarico svolto o da svolgere, al compenso pattuito, alle caratteristiche del rapporto ed alle prassi vigenti; è altresì vietato minacciare i fornitori di ritorsioni qualora effettuino prestazioni a favore di Società concorrenti o utilizzino i servizi di tali Società;
- l'affidamento di un incarico ai consulenti risponda ad obbiettive esigenze della Società, che possono consistere nella necessità di ricevere prestazioni specialistiche, di acquisire competenze mancanti o di integrare competenze esistenti all'interno dell'organizzazione aziendale;
- il pagamento del corrispettivo sia effettuato previa verifica dell'avvenuto espletamento dell'incarico affidato.

D. Gestione dei rapporti con i terzi (es. agenti)

La Società si avvale di agenti e/o consulenti per la ricerca di opportunità commerciali, che intrattengono rapporti diretti anche con la Pubblica Amministrazione Per tale ragione, si è ritenuto opportuno definire norme di comportamento nella gestione dei rapporti con agenti e consulenti – e terze parti in genere – per la prevenzione dei reati contro la Pubblica Amministrazione.

Con riferimento a tale processo sensibile, è fatto obbligo ai Destinatari del Modello di osservare i seguenti protocolli:

- gli agenti e consulenti devono essere scelti in modo trasparente, previa due-diligence e verifica del possesso dei requisiti di competenza, onorabilità e professionalità;
- i rapporti con tali soggetti sono regolati da contratti definiti per iscritto in tutte le loro condizioni e termini, utilizzando gli appositi standard contrattuali; detti contratti contengono "*clausole 231*";
- coerentemente con le *policy* del Gruppo, gli agenti e/o consulenti sono tenuti ad accettare espressamente e sottoscrivere il Codice Etico e il Codice di Condotta Anticorruzione del Gruppo;
- i contratti con gli agenti e con i consulenti devono essere sottoscritti da persone munite dei necessari poteri in conformità alle procedure aziendali;
- il contratto dovrà contenere la dettagliata descrizione delle attività affidate e l'obbligo per l'Agente/Consulente di fornire report regolari e dettagliati che descrivano i servizi resi, le attività espletate e i risultati ottenuti;
- Il contratto deve includere, salvo il caso di retribuzione fissa mensile, i criteri espliciti, oggettivi e adeguati della maturazione del diritto al compenso, la possibilità per il Consulente di emettere fattura solo a ricevimento di BEF (benestare emissione fattura), la durata massima fissata in 1 anno, senza possibilità di rinnovo tacito; l'accettazione da parte del Consulente del MOG 231 e suoi allegati e la dichiarazione del Consulente di assenza di conflitto di interessi;
- il rimborso delle spese, qualora contrattualmente previsto, dovrà essere subordinato alla presentazione dei giustificativi di spesa fiscalmente validi ed al controllo sulla completezza e coerenza dei giustificativi medesimi con la richiesta di rimborso ad opera dell'Amministrazione;
- il corrispettivo per l'Agente e/o Consulente dovrà essere determinato sulla base di criteri chiari, espliciti ed oggettivi;
- i pagamenti a favore di terze parti e, in particolare, degli agenti e/o consulenti possono essere effettuati solo per i servizi concordati in precedenza per iscritto, previa verifica che siano stati effettivamente resi e che siano adeguatamente documentati;
- tutti i pagamenti a favore di terzi (es. agenti) devono essere effettuati esclusivamente tramite bonifico bancario sul conto corrente indicato dal terzo e riportato espressamente nel contratto.

E. Gestione di incassi e pagamenti e tesoreria

In relazione alla gestione dei flussi finanziari e della cassa aziendale:

- è fatto divieto di effettuare pagamenti a terzi che non trovino adeguata giustificazione in relazione al tipo di incarico svolto;
- è fatto divieto di promettere o versare somme di denaro al Funzionario Pubblico a titolo personale con finalità di promuovere o favorire interessi di AXIANS, anche a seguito di illecite pressioni;
- i flussi finanziari (incassi e pagamenti) devono essere gestiti e regolarmente registrati attraverso i sistemi gestionali aziendali in modo da poter essere tracciati e ricostruiti ex post;
- è necessario verificare la corrispondenza tra accordi, ordini di acquisto, fatturazioni e pagamenti relativi anche alle somme da versare, prestando attenzione alle autorizzazioni richieste per potere effettuare i pagamenti;
- nessun pagamento può essere effettuato in contanti, salvo quelli compresi nella gestione della piccola cassa;
- è fatto assoluto divieto di compiere qualsiasi operazione volta alla creazione di fondi extracontabili.

F. Gestione dei rimborsi spese a dipendenti e collaboratori, comprese eventuali spese di rappresentanza

In aggiunta a quanto previsto dalla "PURU10_*Travel Policy*", dalla "*PURU03_Procedura Gestione e Sviluppo delle Risorse Umane*" e dalla procedura "*PMOG03_Gestione Omaggi e Inviti*":

- spese di rappresentanza, pranzi/cene ed ospitalità (es. spese per vitto e alloggio sostenute a favore di terzi in occasione di attività aziendali) sono ammesse nei limiti del budget approvato annualmente dal CdA e previa autorizzazione da parte dei soggetti dotati di adeguati poteri, qualora queste spese superino le soglie determinate da VINCI Energies e indicate nel documento "*Guidelines Omaggi e Inviti Vinci Energies Italia*";
- il *BU Manager* ha il potere di determinare le ospitalità e le spese relative a pranzi/cene professionali, ma sempre nei limiti del budget assegnato alla BU di appartenenza e secondo i criteri indicati nelle "*Guidelines Omaggi e Inviti Vinci Energies Italia*" e riportati nella procedura interna "*PMOG03_Gestione Omaggi & Inviti*";
- sono ammesse spese di rappresentanza di modico valore e che siano funzionali all'attività svolta da AXIANS; in particolare, tali spese possono essere finalizzate unicamente ad accrescere l'immagine della Società e in nessun modo possono avere lo scopo di condizionare il compimento di attività da parte di soggetti pubblici o privati;
- ogni spesa deve essere documentata e rendicontata in modo veritiero e trasparente anche attraverso gli strumenti messi a disposizioni dal gruppo;
- il rimborso delle spese è subordinato alla presentazione dei giustificativi di spesa fiscalmente validi ed al controllo sulla completezza e coerenza dei giustificativi medesimi con la richiesta di rimborso ad opera dell'Amministrazione;
- al fine di garantire la tracciabilità dei rimborsi spese non è consentito erogare il rimborso in denaro contante, salvo in casi eccezionali e fermo restando l'obbligo per il richiedente di allegare i giustificativi di spesa;
- l'ufficio HR payroll verifica la corretta rendicontazione della nota spesa incrociando le indicazioni della travel policy con i dati inseriti nella nota spesa e sul timesheet;
- l'amministrazione verifica, da un punto di vista fiscale, la correttezza dei giustificativi caricati dal dipendente, creando un file con l'indicazione degli importi da rimborsare o trattenere sul cedolino.
- tutta la documentazione relativa ai rimborsi spese è conservata a cura dell'Amministrazione in apposito archivio cartaceo o telematico.

G. Gestione delle sponsorizzazioni e concessione di donazioni, omaggi e liberalità

Conformemente a quanto previsto dalle Procedure "*PMOG03_Gestione Omaggi & Inviti*" e "*PMOG04_Gestione dei rapporti con la PA*":

- è vietato ricevere e/o accettare omaggi e liberalità da parte di Terzi salvo previa autorizzazione del proprio Responsabile e nei limiti di quanto consentito nella Procedura Omaggi;
- omaggi, sponsorizzazioni e liberalità a favore di terzi devono essere autorizzati da un soggetto

diverso dal proponente, essere coerenti con il budget di funzione assegnato dal CdA e, in ogni caso, documentati;

- salvo espressa autorizzazione di un amministratore, gli omaggi devono essere di modico valore;
- non possono essere effettuate donazioni, omaggi o regalie in forma di denaro contante o equivalenti, indipendentemente dall'importo;
- sponsorizzazioni e liberalità possono essere deliberate esclusivamente dall'organo amministrativo (CdA o AD munito dei necessari poteri), eventualmente su richiesta del *BU Manager*; gli omaggi sono decisi dal *BU Manager* in coerenza con il budget assegnato alla BU e secondo i criteri indicati nelle "*Guidelines Omaggi e Inviti Vinci Energies Italia*" e riportati nella procedura interna "*PMOG03_Gestione degli omaggi, liberalità, sponsorizzazioni ed ospitalità*";
- è vietata ogni forma di liberalità, diretta e/o indiretta, finalizzata ad influenzare le scelte della PA o a sensibilizzarne gli appartenenti;
- è vietata ogni forma di regalia o liberalità su iniziativa personale o attingendo a fondi propri o sociali non previamente adibiti a tale scopo; parimenti, è vietato concedere regalie o liberalità su richiesta del Pubblico Ufficiale o dell'Incaricato di pubblico servizio;
- gli omaggi e i gadget possono essere acquistati esclusivamente dal Responsabile Acquisti, il quale verificherà che la richiesta sia stata autorizzata e che la spesa sia coerente con il budget assegnato alla BU di riferimento;
- il personale che intenda concedere omaggi o ospitalità a terzi per un valore o una periodicità superiori alle soglie indicate nelle "*Guidelines Omaggi e Inviti Vinci Energies Italia*" e riportati nella procedura interna "*PMOG03_Gestione degli omaggi, liberalità, sponsorizzazioni ed ospitalità*" deve richiedere l'autorizzazione al proprio *BU Manager* ,riportando la descrizione dell'omaggio o ospitalità, il suo costo unitario, la quantità, il nominativo dell'ente beneficiario e la data dell'erogazione; Il *BU Manager* esamina la richiesta del proponente ed eventualmente la approva, previa verifica del rispetto delle regole definite dalla procedura "*PMOG03_Gestione Omaggi & Inviti*". In caso di approvazione, il Responsabile Acquisti ed il Responsabile Amministrazione daranno seguito alle richieste previa verifica della coerenza dell'omaggio/ospitalità con il *budget* di funzione e della sussistenza delle necessarie autorizzazioni; al fine di garantire la massima tracciabilità dell'operazione, gli omaggi e le liberalità elargite devono risultare nella contabilità aziendale nonché segnalati attraverso gli strumenti messi a disposizioni dal gruppo;
- le sponsorizzazioni devono essere disposte previa identificazione dell'Ente beneficiario e acquisizione di informazioni sull'affidabilità dello stesso e sulla coerenza con l'attività svolta dalla Società;
- le sponsorizzazioni devono essere deliberate dal CdA ed essere disciplinate contrattualmente, nel rispetto dei principi del presente Modello, dei Codici e delle *policy* di Gruppo.

H. Selezione, assunzione e gestione del personale

In relazione al processo di selezione, assunzione e gestione del personale (es. promozioni, avanzamenti di carriera, aumenti, assegnazione di "*fringe benefits*", ecc.) le procedure aziendali e, in particolare, le procedure "*PURU01_Gestione della ricerca e selezione del personale*" e "*PURU03_Gestione e sviluppo delle risorse umane*", e le *policy* di Gruppo stabiliscono che:

- la selezione del personale deve essere gestita secondo i criteri di trasparenza e imparzialità;

- è vietato tenere comportamenti discriminatori ed effettuare favoritismi in fase di selezione, assunzione, nonché nella gestione degli aumenti salariali, incentivi e promozioni;
- sussiste una chiara definizione dei ruoli e dei compiti dei soggetti responsabili della selezione e della gestione dei rapporti con i dipendenti;
- l'assunzione di una nuova risorsa risponde ad esigenze interne obiettive e verificabili;
- la selezione avviene previa acquisizione del *curriculum vitae* del candidato, svolgimento di almeno due colloqui attitudinali, valutazione del candidato sulla base di criteri predefiniti e obiettivi (quali professionalità, preparazione e attitudine alle mansioni); la scelta del candidato deve essere espressamente motivata e approvata dal BU Manager e dal Responsabile della funzione di riferimento;
- è garantita la tracciabilità delle motivazioni che hanno indotto alla scelta o all'esclusione del candidato;
- viene effettuata una verifica di eventuali situazioni di conflitti di interesse in capo al candidato,
- sottoponendo allo stesso, in sede di primo colloquio, un apposito modulo ("*Scheda Candidato*") nel quale si richiede di specificare se sono stati precedentemente svolti incarichi presso la PA, se vi sono legami di parentela/coniugio con esponenti della PA o dipendenti della Società o se il candidato o un suo familiare stretto ha svolto ruoli apicali per un nostro concorrente o fornitore;
- Ogni dipendente, non appena venga a conoscenza di una situazione di conflitto di interesse, effettivo o potenziale, propria o di un proprio parente/soggetto vicino, deve darne **tempestiva comunicazione scritta** al proprio responsabile diretto, e comunque **entro 7 giorni** da quando ne è venuto o avrebbe dovuto ragionevolmente venirne a conoscenza;
- al termine del processo di selezione, il candidato è sottoposto ad una verifica circa il possesso dei requisiti di onorabilità attraverso la richiesta di un'autodichiarazione relativa all'assenza di precedenti penali o carichi pendenti per i reati previsti dal D.Lgs. 231/2001;
- in fase di assunzione, al candidato è richiesto di sottoscrivere un contratto contenente clausole di accettazione del Codice Etico e del Codice Anticorruzione di Gruppo, nonché del Modello 231 della Società; inoltre, i dipendenti, che per ruolo o mansione, possano essere coinvolti in eventi corruttivi, sono tenuti ad accettare espressamente i Codici di Gruppo, che gli stessi devono sottoscrivere accedendo con le proprie credenziali al portale dedicato (*Cometh*);
- tutta la documentazione relativa al processo di selezione e gestione del personale è archiviata a sistema a cura della funzione Risorse Umane;
- viene regolarmente erogata attività formativa ai dipendenti/collaboratori in materia di anticorruzione e, in generale, sul D. Lgs. 231/2001;
- è fatto divieto di promettere ingiustificati avanzamenti di carriera (passaggi di qualifica, aumenti retributivi e *fringe benefit*);
- eventuali avanzamenti di carriera, premi e incentivi devono essere basati su valutazioni oggettive in merito alle competenze possedute e a quelle potenziali, nonché alle *performace* svolte, alla luce dei criteri e delle regole enunciate dalla "*PURU03 Gestione e sviluppo delle risorse umane*";
- la proposta di avanzamento di carriera richiede la verifica e l'approvazione da parte del BU Manager e dell'Amministrazione Delegato, eventualmente anche con il supporto di Finance;
- è assicurata la tracciabilità dei sistemi di retribuzione e incentivazione.

5. Reporting all'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di verificare la corretta applicazione dei protocolli di cui alla presente Parte Speciale, i Responsabili delle Funzioni coinvolte nella gestione dei processi sensibili di cui al punto 2) della presente Sezione dovranno trasmettere all'OdV le informazioni e le segnalazioni previste dalle procedure "*PMOG02 ODV Procedura Flussi informativi*" e "*PMOG01 Procedura Segnalazione Violazioni Whistleblowing*".

Parte speciale 2

Omicidio colposo e lesioni personali colpose commessi con violazione delle norme antinfortunistiche e di tutela dell'igiene e della salute sul lavoro

La presente Parte Speciale si riferisce ai reati realizzabili in materia di tutela della salute e della sicurezza sui luoghi di lavoro, come dettagliatamente definiti nell'**Allegato A**.

1.I reati in materia di salute e sicurezza sui luoghi di lavoro (art. 25-septies del D.Lgs. 231/01)

In considerazione della mappatura dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati:

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

Per una disamina approfondita dei reati sopra elencati e delle sanzioni applicabili all'ente si rimanda all'**Allegato A**.

2. Attività sensibili

Con riferimento ai reati di cui all'art. 25-septies del Decreto, i processi considerati maggiormente a rischio, sono i seguenti:

A) gestione degli adempimenti in materia di salute e sicurezza degli impianti e dei luoghi di lavoro;
B) affidamento di lavori in appalto e subappalto;
C) gestione di lavori che comportino l'adozione di cantieri.

Le norme antinfortunistiche e di tutela dell'igiene e della salute sul lavoro previste dal D.Lgs. 81/2008 (Testo Unico sulla Sicurezza sul Lavoro – T.U.S.L.) e le disposizioni di cui alla presente parte speciale hanno come Destinatari tutti i soggetti della sicurezza, ossia: il datore di lavoro, i dirigenti, i preposti ed i lavoratori; il responsabile del servizio di prevenzione e protezione (**RSPP**), il Responsabile del Sistema di Gestione sulla Sicurezza (**RSGS**), gli Addetti al Servizio di Prevenzione e Protezione (**ASPP**), il medico competente (**MC**), nonché agli addetti al primo soccorso e agli addetti emergenze in caso d'incendio.

In caso di allestimento di cantieri temporanei o mobili, alcune specifiche disposizioni si applicano al committente, al rappresentante dei lavoratori per la sicurezza (**RLS**) e i coordinatori per la sicurezza.

In particolar modo, il presente Modello prevede l'adozione e l'efficace attuazione degli obblighi

giuridici che l'art. 30 del D. Lgs. 81/01 prevede quali esimenti della responsabilità amministrativa degli enti disciplinata dal Decreto, ossia:

- il rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

- l'espletamento dell'attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;

- l'espletamento delle attività di natura organizzativa volte alla prevenzione della salute e sicurezza sul lavoro, quali gestione delle emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza e consultazioni dei rappresentanti dei lavoratori per la sicurezza;

- l'espletamento dell'attività di sorveglianza sanitaria;

- l'implementazione delle attività di informazione e formazione dei lavoratori;

- l'attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

- l'acquisizione di documentazioni e certificazioni obbligatorie di legge;

- lo svolgimento di periodiche verifiche circa l'applicazione e l'efficacia delle procedure adottate.

Il presente Modello garantisce un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio.

La Società garantisce il rispetto del presente Modello attraverso l'adozione di un sistema di controllo che assicuri l'attuazione dei presidi adottati e il mantenimento nel tempo delle condizioni di idoneità delle misure di prevenzione e altresì preveda sistemi di registrazione dell'avvenuta effettuazione delle attività di prevenzione nonché un sistema disciplinare volto a sanzionare il mancato rispetto delle misure prescritte.

La società individua la normativa in materia di salute e sicurezza applicabile alla società, pianifica gli interventi necessari per verificarne il rispetto, individua le funzioni aziendali competenti preposte all'organizzazione dei controlli periodici nei casi previsti dalla legge, al periodico monitoraggio dello stato dei dispositivi di sicurezza, di attrezzature, macchine ed impianti, alla segnalazione delle eventuali non conformità riscontrate e all'attuazione di conseguenti interventi manutentivi.

La società si attiva tempestivamente all'adeguamento e al miglioramento dei presidi adottati in caso di 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. Infine, secondo quanto previsto dall'art. 30 comma 3 del Decreto medesimo

la Società definisce le modalità per individuare e sanzionare comportamenti che costituiscono o che possono favorire la violazione/elusione del sistema di controllo, il mancato rispetto delle procedure e prescrizioni previste dal Modello, il mancato rispetto degli obblighi previsti dalla legislazione in materia di salute e sicurezza, la commissione di reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro e adotta un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel presente Modello.

Il tipo e l'entità delle sanzioni potranno essere determinati, ad esempio, in relazione all'intenzionalità del comportamento, alla rilevanza della violazione di norme o disposizioni, al grado di negligenza, imprudenza o imperizia, al livello delle responsabilità connesse alle mansioni attribuite, al tipo di conseguenze.

L'azienda definisce altresì idonee modalità per selezionare, monitorare ed eventualmente sanzionare collaboratori esterni, appaltatori, fornitori e altri soggetti aventi rapporti contrattuali con l'azienda stessa *Perché tali modalità siano applicabili l'azienda deve prevedere che nei singoli contratti siano inserite specifiche clausole applicative con riferimento ai requisiti e comportamenti richiesti ed alle sanzioni previste per il loro mancato rispetto, fino alla risoluzione del contratto stesso*.

Al fine di prevenire la commissione dei reati in materia di salute e sicurezza sul lavoro, la Società si è dotata di una struttura organizzativa conforme a quella prevista dalla normativa vigente di cui al D. Lgs. 81/2008 e successive modifiche. In particolare, la Società ha adottato un Sistema di Gestione della Sicurezza (**SGS**) conforme allo standard UNI EN ISO 45001:2018, integrato con il Sistema di Gestione della Qualità e della Sicurezza delle informazioni.

AXIANS si è altresì dotata di un sistema di deleghe e procure in materia di sicurezza adeguato e conforme alle disposizioni di cui al D. Lgs 81/2008. In particolare, il Consiglio di Amministrazione ha designato al suo interno il Datore di Lavoro, attribuendo tale ruolo all'Amministratore Delegato, il quale, a sua volta, ha nominato i singoli *BU Manager* datori di lavoro delegati ai sensi dell'art. 16 del D.Lgs. 81/2008.

È stata inoltre istituita una funzione *QHSE Specialist* ed è stato nominato un RSPP esterno.

Per una disamina completa e dettagliata dei ruoli e delle responsabilità in materia di salute e sicurezza sul lavoro si rimanda all'organigramma societario sulla sicurezza IDGS03-I, pubblicato nella cartella sharepoint aziendale.

L'attività eventualmente appaltata, anche in subappalto, ad aziende esterne è seguita con particolare attenzione; gli appaltatori/subappaltatori devono essere scelti in ragione della loro comprovata capacità e devono essere sensibilizzati ad operare mediante la puntuale osservanza delle norme che disciplinano la salute e la sicurezza sui luoghi di lavoro.

La società non commissiona attività ex Titolo IV (cantieri mobili o temporanei) ma opera presso cantieri edili e navali come appaltatrice/subappaltatrice. I principali rischi per la salute e la sicurezza dei lavoratori sono collegati alle attività di installazione e/o manutenzione di impianti eseguite presso tali

cantieri. A titolo esemplificativo, si configurano i seguenti rischi: investimento, caduta dall'alto, rischio elettrico, rischi fisici ordinari (caduta, taglio, ecc.).

A fine di eliminare o, quantomeno, ridurre i rischi per i lavoratori, è stato predisposto il documento di valutazione dei rischi (**DVR**) che ha analizzato ogni ipotetico rischio che i lavoratori potrebbero dover affrontare; tale documento è soggetto a modifiche, qualora le esperienze maturate suggeriscano la necessità di implementare il livello di sicurezza in ambito aziendale.

AXIANS, infine, si adopera al fine di promuovere l'attività di informazione e formazione dei lavoratori che viene svolta puntualmente per dare attuazione, nel modo più ampio e completo possibile, al rispetto della legislazione in materia di salute e sicurezza sul lavoro; vengono svolti puntualmente corsi di aggiornamento; viene prestata, inoltre, particolare attenzione affinché ogni lavoratore sia provvisto ed utilizzi i dispositivi di protezione individuale (**DPI**) previsti dalla legislazione.

3. Principi generali di comportamento

Le seguenti disposizioni di carattere generale si applicano, secondo le attribuzioni, i compiti e le responsabilità assegnate, a tutti i soggetti identificati *sub* 2), nonché ai consulenti, fornitori, appaltatori, subappaltatori e partner in forza di apposite clausole contrattuali.

Detti soggetti, ognuno nell'ambito di propria competenza, devono garantire:

a) la definizione degli obiettivi per la sicurezza e la salute dei lavoratori e l'identificazione continua dei rischi;
b) un adeguato livello di informazione/formazione dei dipendenti e dei fornitori/appaltatori/subappaltatori, sul sistema di gestione della sicurezza e salute definito da AXIANS e sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole di comportamento e controllo definite dalla stessa;
c) la definizione e l'aggiornamento (in base a cambiamenti nella struttura organizzativa ed operativa della Società) di procedure specifiche per la prevenzione di infortuni e malattie, in cui siano, tra l'altro, disciplinate le modalità di gestione degli incidenti e delle emergenze, nonché dei segnali di rischio/pericolo, quali i c.d. "*near miss*" o "*quasi incidenti*";
d) l'idoneità delle risorse, sia umane - in termini di numero, qualifiche professionali e formazione specifica - che materiali – in termini di apparecchiature, attrezzature di lavoro e macchinari - necessarie al raggiungimento degli obiettivi prefissati dalla Società per la sicurezza e la salute dei lavoratori;
e) la manutenzione ordinaria e straordinaria degli strumenti, degli impianti e, in generale, delle strutture aziendali.

Per quanto riguarda la gestione degli appalti e dei fornitori, nei contratti di appalto (o subappalto) intesi come contratto di appalto d'opera, di servizi o contratto d'opera o di somministrazione, il Datore di Lavoro in caso di affidamento di lavori, servizi e forniture all'impresa appaltatrice o a Lavoratori autonomi all'interno della propria azienda o unità lavorativa, in conformità alle procedure aziendali, e sempre che abbia la disponibilità giuridica dei luoghi in cui si svolge l'appalto o la prestazione di lavoro autonomo, è chiamato a:

f) verificare, con il supporto delle Unità interessate, l'idoneità tecnico-professionale delle imprese appaltatrici o dei Lavoratori autonomi in relazione alle attività da affidare in appalto;
g) mettere a disposizione degli appaltatori informazioni dettagliate circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
h) cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
i) coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, attraverso un costante scambio di informazioni con i datori di lavoro delle imprese appaltatrici anche al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva. Il Datore di Lavoro committente promuove la cooperazione ed il coordinamento di cui ai punti precedenti elaborando (nei casi previsti dalla legge) un Documento Unico di Valutazione dei Rischi per le Interferenze (**DUVRI**) nel quale siano indicate le misure adottate per eliminare o, laddove non sia possibile, per ridurre al minimo i rischi da interferenze.

Inoltre, è fatto espresso divieto a tutti i soggetti sopra individuati di:

j) 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-septies del D.Lgs. 231/2001);
k) porre in essere o dare causa a violazioni dei principi comportamentali e delle procedure aziendali.

In generale, tutti i soggetti sopra individuati devono rispettare gli obblighi previsti dal D.lgs. 81/2008 e le *policy* definite dal Gruppo, al fine di preservare la salute e la sicurezza dei lavoratori e comunicare tempestivamente, alle strutture individuate e nelle modalità definite nelle procedure aziendali, eventuali segnali di rischio/pericolo (ad esempio, i "*quasi incidenti*"), incidenti (indipendentemente dalla loro gravità) e violazioni alle regole di comportamento e alle procedure aziendali.

4. Protocolli specifici di comportamento

Ad integrazione ed ai fini di fornire un dettaglio operativo rispetto ai principi già declinati nel Codice Etico e Guida ai Diritti Umani, sono state formalizzate specifiche procedure e norme aziendali aventi ad oggetto il sistema di gestione della sicurezza, in particolare:

- la politica e il manuale del Sistema di Gestione della Salute e Sicurezza;
- la procedura per la gestione delle situazioni di rischio e prevenzione delle situazioni di pericolo;
- la procedura per la gestione delle situazioni di emergenza;
- la procedura per l'approvvigionamento di beni, servizi e prestazioni;
- Policy Vinci "Azioni imprescindibili e fondamentali nel campo della salute e della sicurezza sul lavoro";
- Procedure del SGS:
  - PDGS02_Valutazione rischi;
  - PDGS11_Gestione trasferte estero;

- PRO08_Gestione lavori;
- PDSG07_Gestione dispositivi di protezione individuali;
- PRO06_Gestione della protezione delle aree di rilevante importanza;
- PRO05_Gestione degli Audit interni;
- PURU02_Gestione della comunicazione, informazione e formazione;
- PDSG05_Sorveglianza sanitaria;
- PDSG06_Gestione mezzi, attrezzature e strumenti;
- 4_Gestione delle emergenze;
- PRO08_Gestione Lavori;
- IDGS28_Istruzione Operativa per utilizzo Spray scorrimano al silicone
- IDGS27_Istruzione Operative per utilizzo Tappeto in gomma antiolio copritombino
- IDGS26_Istruzione Operativa per utilizzo svitol
- IDGS25_Istruzione Operativa per utilizzo Olio taglio
- IDGS24_Istruzione Operative per utilizzo Alcool Isopropilico
- IDGS23_Istruzione di sicurezza sblocco cancello parcheggio superiore_VI
- IDGS22_Istruzione di sicurezza in caso di sversamento acido batterie__SOLFONET-C
- IDGS21_Istruzione Operativa per utilizzo Spray scorrimano al silicone
- IDGS20_Istruzione Operative per utilizzo Tappeto in gomma antiolio copritombino
- IDGS19_Istruzione Operativa per utilizzo svitol
- IDGS18_Istruzione Operativa per utilizzo Olio taglio
- IDGS17_Istruzione operativa gestione informazioni Trasferte Estero
- IDGS16_Istruzione Operativa per la Movimentazione Manuale di Bobine
- IDGS15_Istruzione Operativa per la Gestione dei Rifiuti
- IDGS14_Istruzione Operativa per l'utilizzo di scale fisse
- IDGS13_Istruzione Operativa in caso di blocco ascensore VI
- IDGS12_Istruzioni per Trasportatori
- IDGS10_Istruzione di Sicurezza per Carico - Scarico Automezzi
- IDGS09_Istruzioni di Sicurezza carica batteria carrello elevatore
- IDGS08_Istruzione per Carico e Scarico Materiali dal Soppalco del Magazzino
- IDGS06_Istruzione Operativa per l'utilizzo di scale portatili
- IDGS05_Piano di Emergenza - filiale di VICENZA
- IDGS03_Piano di Emergenza - filiale di CORSICO (MI)
- IDGS03_Piano di Emergenza - filiale di ROMA via Bianchini
- IDGS03_Piano di Emergenza - filiale di MASSA
- IDGS03_Piano di Emergenza - filiale di TRENTO
- IDGS03_Piano di Emergenza - filiale di CAMPOFORMIDO
- IDGS03_Piano di Emergenza - filiale di ROMA via Tevere
- IDGS03_Piano di Emergenza - filiale di TORINO
- IDGS03_Piano di Emergenza - filiale DI VENEZIA
- IDGS01_Analisi cause infortuni - incidenti - near miss

In aggiunta a tali presidi di controllo, si prevedono i seguenti ulteriori protocolli specifici di comportamento:

A. Gestione degli adempimenti in materia di salute e sicurezza degli impianti e dei luoghi di lavoro

In conformità a quanto previsto dalle procedure aziendali e dalle *policy* di Gruppo richiamate, si prevede che:

- il RSPP, il Medico Competente, gli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, nonché i Dirigenti e i Preposti (ove nominati) sono designati formalmente, tramite lettera d'incarico sottoscritta dall'interessato;
- il RSPP organizza la riunione periodica sulla sicurezza in conformità a quanto previsto dall'art. 35 del T.U.S.L., redige e fa sottoscrivere un verbale, mettendolo a disposizione dei partecipanti per la sua consultazione;
- al fine di garantire un costante monitoraggio delle misure preventive e protettive predisposte per la tutela della salute e sicurezza sui luoghi di lavoro, nonché dell'adeguatezza e della funzionalità del SGS a raggiungere gli obiettivi prefissati e della sua corretta applicazione, il *QHSE Manager*, l'RSPP e il *General Services Manager* effettuano regolarmente sopralluoghi per verificare il rispetto delle norme comportamentali sull'ambiente di lavoro;
- gli esiti delle verifiche di cui sopra sono formalizzati compilando l'apposita *check list* e predisponendo un verbale delle operazioni espletate;
- ogni infortunio o "*quasi infortunio*" viene puntualmente analizzato e registrato, al fine di individuare eventuali lacune nel sistema di tutela della salute e della sicurezza e di identificare le conseguenti azioni correttive da intraprendere;
- sono conservati i manuali e le istruzioni per l'uso di macchinari, attrezzature e dispositivi di protezione individuale e viene mantenuto uno scadenziario delle attività di manutenzione ordinaria da effettuare;
- l'attività di formazione e informazione dei lavoratori in materia di salute e sicurezza sui luoghi di lavoro è garantita dall'organizzazione di corsi di formazione specifica, all'esito dei quali ciascun lavoratore viene sottoposto a verifiche di apprendimento; l'informazione sui rischi collegati alle specifiche mansioni viene fornita anche attraverso apposita "*Scheda informazione/mansione*";
- tutta la documentazione relativa alla formazione/informazione è conservata a cura di QHSE-ASPP e messa a disposizione dell'Organismo di Vigilanza a semplice richiesta;
- è stata regolarmente attivata la sorveglianza sanitaria e nominato il Medico Competente; quest'ultimo visita almeno una volta l'anno tutti gli ambienti di lavoro dell'azienda e redige apposito verbale ("*Verbale sopralluogo Medico Competente*");
- la cartella sanitaria è istituita, aggiornata e custodita dal Medico Competente; una copia viene annualmente consegnata al Datore di Lavoro, che la custodisce come per legge;

Inoltre:

- I <u>Fornitori</u> devono rispettare il divieto di fabbricare, vendere, noleggiare e concedere in uso di attrezzature di lavoro, dispositivi di protezione individuali ed impianti non rispondenti alle disposizioni legislative e regolamentari vigenti in materia di salute e sicurezza sul lavoro. In caso di locazione finanziaria di beni assoggettati a procedure di attestazione alla conformità, gli stessi debbono essere accompagnati, a cura del concedente, dalla relativa documentazione;
- I <u>Progettisti</u> dei luoghi e dei posti di lavoro e degli impianti rispettano i principi generali di prevenzione in materia di salute e sicurezza sul lavoro al momento delle scelte progettuali e tecniche e scelgono attrezzature, componenti e dispositivi di protezione rispondenti alle disposizioni legislative e regolamentari in materia;

- Gli Installatori e montatori di impianti, attrezzature di lavoro o altri mezzi tecnici, per la parte di loro competenza, devono attenersi alle norme di salute e sicurezza sul lavoro, nonché alle istruzioni fornite dai rispettivi fabbricanti.

B. Affidamento di lavori in appalto

In caso di affidamento dei lavori, servizi e forniture, contratti d'opera o somministrazione presso le filiali della Società ad imprese o lavoratori autonomi che non comportino l'obbligo di adozione di cantieri temporanei o mobili, AXIANS:

- si impegna all'osservanza delle disposizioni di legge in materia di salute e sicurezza dei lavoratori in caso di appalto di cui al D.Lgs. 81/2008;
- predispone e mantiene aggiornato un elenco delle aziende con le quali stipula eventuali contratti di appalto;
- definisce le modalità di gestione e di coordinamento dei lavori in appalto per iscritto, in contratti dai quali devono risultare espressi riferimenti agli adempimenti di cui all'art. 26 del T.U.S.L.;
- nei contratti di appalto di cui al punto precedente, deve essere chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro anche nel caso di subappalto.

In ogni caso, gli appaltatori, i fornitori e i lavoratori autonomi hanno l'obbligo di osservare quanto stabilito nel documento di valutazione dei rischi interferenziali (**DUVRI**).

C. Gestione di lavori che comportino l'adozione di cantieri

Con riferimento agli affidamenti di appalti o lavori che comportino l'adozione di cantieri temporanei o mobili cantieri, come definiti dall'art. 89 del T.U.S.L., premesso che AXIANS agisce esclusivamente in qualità di appaltatrice o subappaltatrice, la stessa si impegna ad osservare le disposizioni contenute del Titolo IV del D.Lgs 81/2008:

- effettuare una dettagliata analisi di tutti i rischi per la salute e sicurezza dei lavoratori;

- eliminare i rischi, ove possibile;

- dare adeguata informazioni e formazione ai lavoratori, dirigenti e preposti, predisponendo anche le misure di emergenza da attuare in caso di primo soccorso;

- qualora rivesta la qualifica di committente, designare il coordinatore per la progettazione e il coordinatore per l'esecuzione dei lavori;

- verificare l'idoneità tecnico-professionale delle imprese affidatarie e delle imprese esecutrici;

- richiedere una dichiarazione dell'organico annuo alle imprese esecutrici, assicurare la presentazione di un POS di un Fascicolo dell'Opera e la predisposizione di un PSC e osservare

ogni altra disposizione in materia di cantieri.

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'OdV.

In particolare, nelle ipotesi in cui i lavoratori di AXIANS si trovino ad operare presso cantieri di clienti terzi committenti, la Società si impegna a:

- effettuare una dettagliata analisi di tutti i rischi per la salute e sicurezza dei lavoratori, redigendo apposito Piano Operativo di Sicurezza (**POS**) per ogni cantiere;
- eliminare o ridurre i rischi per la sicurezza e la salute dei lavoratori, ove possibile;
- dare adeguata informazione e formazione ai lavoratori occupati nel cantiere, predisponendo anche le misure di emergenza da attuare in caso di primo soccorso.

5. Reporting all'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di verificare la corretta applicazione dei protocolli di cui alla presente Parte Speciale, i Responsabili delle Funzioni coinvolte nella gestione dei processi sensibili di cui al punto 2) dovranno trasmettere all'OdV le informazioni e le segnalazioni previste dalle procedure "*PMOG02 ODV Procedura Flussi informativi*" e "*PMOG01 Procedura Segnalazione Violazioni Whistleblowing*".

Parte Speciale 3

Reati Societari

La presente Parte Speciale si riferisce ai reati societari di cui all'art. 25-ter del Decreto, come dettagliatamente definiti nell'**Allegato A**.
I reati societari sono reati propri e, in quanto tali, possono essere commessi, a titolo esemplificativo, da amministratori, direttori generali, sindaci, liquidatori, nonché, a titolo di concorso, anche dalle strutture preposte alla gestione di attività amministrativo-contabili, finanziarie o relative all'implementazione del sistema informativo contabile.

1. I reati societari (art. 25-ter del D.Lgs. 231/2001)

In considerazione della mappatura dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati:

- false comunicazioni sociali (art. 2621 c.c.);
- fatti di lieve entità (art. 2621 bis c.c.);
- impedito controllo (art. 2625, comma 2, c.c.);
- indebita restituzione dei conferimenti (art. 2626 c.c.);
- illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- illecite operazioni sulle azioni o quote sociali o della Società controllante (art. 2628 c.c.);
- operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.);
- formazione fittizia del capitale (art. 2632 c.c.);
- indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- illecita influenza sull'assemblea (art. 2636 c.c.);
- aggiotaggio (art. 2637 c.c.);
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.).

Per una disamina approfondita dei reati e delle sanzioni applicabili all'ente si rimanda all'**Allegato A**.

2. Attività sensibili

Con riferimento ai reati di cui all'art. 25-ter del Decreto, i processi considerati maggiormente a rischio sono i seguenti:

A) gestione della contabilità generale e formazione del bilancio, tenuta delle scritture contabili e dei libri sociali;
B) operazioni sul capitale sociale e operazioni straordinarie;

C) gestione delle comunicazioni ai soci, agli organi di controllo (Collegio sindacale e Revisore) e/o a terzi realtive alla situazione economica, patrimoniale e finanziaria della Società
D) gestione dei flussi finanziari.

3. Principi generali di comportamento

I seguenti principi di carattere generale si applicano agli organi sociali, ai dirigenti e ai dipendenti di AXIANS in via diretta, nonché ai consulenti, ai fornitori e ai partner in forza di apposite clausole contrattuali. Conformemente a quanto previsto nel Codice Etico e dalle *policy* di Gruppo, tali soggetti devono agire nel rispetto dei principi di trasparenza, accuratezza e completezza delle informazioni affinché:

- ogni informazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua;
- la rappresentazione della situazione economica, patrimoniale e finanziaria sia veritiera, corretta e trasparente.

Inoltre, è fatto espresso divieto di:

a) porre in essere comportamenti tali da integrare le fattispecie previste dall'art. 25-ter del Decreto;
b) predisporre documenti o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una rappresentazione errata della situazione economica, finanziaria e patrimoniale della Società;
c) omettere di comunicare dati e informazioni imposte dalla legge con riguardo alla situazione economica, patrimoniale o finanziaria;
d) occultare documenti, esibire documentazione contabile parzialmente o alterandola, ostacolando le attività di controllo e di revisione;
e) tenere una condotta ingannevole che possa indurre il Collegio Sindacale o la Società di Revisione in errori di valutazione tecnico-economica della documentazione presentata;
f) influenzare l'assemblea con atti simulati o fraudolenti;
g) acquistare o sottoscrivere quote sociali cagionando lesione all'integrità del capitale sociale o delle riserve;
h) sottoscrivere reciproche quote;
i) sopravvalutare i conferimenti di beni in natura, i crediti o il patrimonio della Società nel caso di trasformazione;
j) restituire anche simulatamente i conferimenti dei soci o liberalizzare gli stessi dall'obbligo di eseguirli;
k) ripartire gli utili o gli acconti sugli utili non effettivamente eseguiti o destinati a riserva;
l) porre in essere azioni volte ad ostacolare o impedire lo svolgimento delle attività di controllo;
m) utilizzare o comunicare ad altri, senza giustificato motivo, le informazioni riservate cui si ha accesso;
n) esporre nelle comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie di AXIANS.

4. Protocolli specifici di comportamento

Ad integrazione ed ai fini di fornire un dettaglio operativo rispetto ai principi già declinati nel Codice

Etico e nel presente Modello, sono state formalizzate specifiche procedure e norme aziendali aventi ad oggetto il sistema di gestione della sicurezza, in particolare:

- PMOG05_Procedura Gestione Flussi Finanziari ed Economici

Si prevedono, inoltre, i seguenti protocolli specifici di comportamento:

A. Gestione della contabilità generale e formazione del bilancio, tenuta delle scritture contabili e dei libri sociali

In relazione alla gestione della contabilità ed alla formazione del bilancio civilistico e consolidato, è fatto obbligo di:

- attenersi ai principi e alle prescrizioni contenute nella normativa di riferimento per la redazione del bilancio e della rendicontazione periodica disciplinata dalla legge;
- osservare tutte le disposizioni previste dalla legge a tutela dell'integrità ed effettività del patrimonio della Società, al fine di non ledere le garanzie dei creditori e dei terzi in genere.

Inoltre, in conformità alle *policy* di Gruppo e alle prassi interne vigenti:

- sono definiti con chiarezza i dati e le notizie che ciascuna funzione deve fornire e i criteri contabili per l'elaborazione dei dati contabili;
- prima della emissione della bozza di bilancio (anche consolidato) occorre verificare la corrispondenza dei documenti alle risultanze dei libri e delle scritture contabili, nonché l'idoneità degli stessi a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria dell'emittente e dell'insieme delle imprese incluse nel consolidamento;
- sono chiaramente individuati i soggetti deputati a gestire per conto della Società la contabilità ed il processo di formazione dei documenti contabili.

B. Operazioni sul capitale sociale e operazioni straordinarie

Eventuali operazioni societarie devono essere condotte in maniera trasparente, veritiera e corretta, coerentemente e nel rispetto dei poteri attribuiti. In particolare:

- deve essere garantita una segregazione di ruoli e responsabilità tra chi evidenzia la necessità di un'operazione, chi la esegue e chi effettua il relativo controllo, anche avvalendosi del supporto di consulenti esterni, ove necessario;
- occorre altresì verificare la sussistenza di eventuali conflitti di interesse in capo alla controparte dell'operazione;
- per ogni documentazione predisposta deve essere assicurata la tracciabilità delle relative fonti e degli elementi informativi;
- tutta la documentazione deve contenere elementi veritieri e coerenti all'oggetto per cui sono stati richiesti;

- la documentazione relativa alle operazioni societarie deve essere opportunamente archiviata.

C. Gestione delle comunicazioni ai soci, agli organi di controllo (Collegio sindacale e Revisore) e/o a terzi realtive alla situazione economica, patrimoniale e finanziaria della Società

Nella gestione dei rapporti con i soci, il Collegio Sindacale e i Revisori, nonché nelle comunicazioni verso l'esterno, devono essere osservate le seguenti disposizioni:

- sono chiaramente identificati i soggetti interni alla Società preposti ad interloquire con gli organi di controllo e a trasmettere agli stessi la documentazione richiesta;
- occorre effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge non frapponendo alcun ostacolo ai controlli delle Autorità di Vigilanza;
- il Collegio Sindacale e il Revisore possono prendere contatti con l'Organismo di Vigilanza per verificare congiuntamente situazioni che possano presentare aspetti di criticità in relazione ai reati societari.

Inoltre, è fatto divieto di:

- omettere di comunicare dati e informazioni richiesti dal Collegio Sindacale o dalla Società di Revisione in relazione alla situazione economica, patrimoniale e finanziaria della Società;
- ostacolare, in qualunque modo, l'esercizio delle funzioni attribuite dalla legge a tali organi.

D. Gestione dei flussi finanziari

In conformità a quanto previsto dalla procedura "*PMOG05 Procedura Gestione Flussi Finanziari ed Economici*":

- le transazioni devono essere tracciabili e verificabili ex post tramite adeguati supporti documentali/informativi;
- è necessario verificare la corrispondenza tra contratti, ordini di acquisto, fatturazioni e pagamenti;
- occorre altresì verificare, anche a campione, la conformità delle fatture alle prescrizioni di legge;
- nessun pagamento può essere effettuato in contanti;
- è fatto assoluto divieto compiere qualsiasi operazione volta alla creazione di fondi extracontabili.

5. Reporting all'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di verificare la corretta applicazione dei protocolli di cui alla presente Parte Speciale, i Responsabili delle Funzioni coinvolte nella gestione dei processi sensibili di cui al punto 2) dovranno trasmettere all'OdV le informazioni e le segnalazioni previste dalle

procedure "*PMOG02 ODV Procedura Flussi informativi*" e "*PMOG01 Procedura Segnalazione Violazioni Whistleblowing*".

axians

Parte Speciale 4

Delitti informatici e trattamento illecito di dati e violazione del diritto d'autore

La presente Parte Speciale si riferisce ai reati informatici e ai delitti commessi in violazione del diritto d'autore di cui agli artt. 24-bis e 25-novies del Decreto, come dettagliatamente definiti nell'**Allegato A**.

1. I reati informatici, trattamento illecito di dati e violazione del diritto d'autore (artt. 24-bis, 25-novies e 25-vicies del D.Lgs. 231/2001)

In considerazione della mappatura dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati:

- Omessa adozione di misure di sicurezza o sorveglianza su IA ad alto rischio (Art. 437-bis c.p.);

- falsità in documenti informatici (art. 491-bis c.p.);

- Diffusione illecita di deepfake (Art. 612-quater c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);
- estorsione c.d. informatica (art. 629 comma 3 c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico di cui (art. 635 quater.1 c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.).

I delitti sopra considerati presuppongono l'utilizzo della rete informatica aziendale, intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi, composta da:

- l'infrastruttura di rete, costituita dalle apparecchiature e dal relativo *software* che consentono i collegamenti all'interno delle sedi aziendali e la connessione da e verso l'esterno dell'azienda;
- i servizi di rete, ossia le *utilities* di carattere generale a disposizione di tutti i dipendenti, distribuite o messe a disposizione centralmente quali, a titolo esemplificativo, servizi di posta elettronica, accesso a internet, anagrafiche centralizzate, ecc.;
- le applicazioni ed i servizi di rete aziendali, che sono resi disponibili agli utenti attraverso i *server*, mentre i punti di accesso alla rete aziendale sono le postazioni di lavoro fisse e mobili assegnate agli utenti stessi.

Per analogia, vengono ricompresi nella presente Parte Speciale anche i delitti in violazione del diritto d'autore di cui all'art. 25-novies del D. Lgs. 231/2001, essendo gli stessi configurabili, nella specifica realtà di AXIANS, soprattutto con riferimento all'attività di installazione e gestione di *software* e *hardware*. In particolare, i reati di cui all'art. 25-novies ritenuti astrattamente applicabili in relazione all'attività esercitata da AXIANS, sono i seguenti:

- messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n. 633/1941 comma 1 lett. a) bis);
- reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n. 633/1941 comma 3);
- abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n. 633/1941 comma 1);
- riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione vendita o concessione in locazione di banche di dati (art. 171-bis legge n. 633/1941 comma 2);
- abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n. 633/1941);
- mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n. 633/1941);

- fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparato o parti di apparati atta alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n. 633/1941).

Con riferimento al reato di estorsione, introdotto nel catalogo dei reati presupposto dall'art. 20, comma 1, lettere a), b), c) della L. 28 giugno 2024, n. 90, sulla base del *risk assessment* effettuato, si è ritenuto di inserirlo relativamente all'ipotesi di concorso nel reato tra l'estorsore e uno dei soggetti apicali dell'azienda.

Per una disamina approfondita dei reati e delle sanzioni applicabili all'ente si rimanda all'**Allegato A**.

2. Attività sensibili

Con riferimento ai reati di cui alla presente Sezione, i processi ritenuti maggiormente a rischio sono i seguenti:

A) gestione e utilizzo dell'infrastruttura tecnologia e dei sistemi informatici e telematici aziendali;
B) gestione di *software* e banche dati.

Le disposizioni della Presente Parte Speciale si applicano a tutti i soggetti aziendali coinvolti, a vario titolo, nella gestione e/o nell'utilizzo dei sistemi informativi aziendali e nell'installazione di *software*, ai collaboratori esterni, temporanei e continuativi, ai fornitori e, in generale, a terze parti che agiscano in nome e per conto della Società e, in ragione dell'attività espletata, abbiano accesso fisico o logico ai sistemi informativi di AXIANS.
In particolare, al fine di prevenire la commissione dei reati informatici, l'accesso alla rete aziendale è consentito solo a indirizzi IP registrati e ogni utente dispone di credenziali di accesso (*user id* e *password*) personali, con scadenza periodica (ogni 6 mesi). Gli accessi al sistema informatico da parte di Terzi sono soggetti alla preventiva autorizzazione dell'*IT Manager* e qualsiasi attività effettuata da tali soggetti sul sistema informatico interno è monitorata e visibile.
La Società ha inoltre adottato un **Sistema di Gestione della Sicurezza delle informazioni certificato ISO 27001** e implementato un **sistema di *Backup* e *Disaster recovery***. La stessa è quindi periodicamente sottoposta ad attività di audit da parte dell'ente certificatore per la verifica della conformità del sistema di gestione delle informazioni allo standard di sicurezza ISO 27001. In occasione di tali verifiche, non sono mai state evidenziate non conformità bloccanti e la certificazione è stata mantenuta nel tempo. Ulteriori audit sull'applicazione delle procedure interne in materia di *cybersecurity* e ITC sono effettuati a cura del personale interno specializzato (es. *Cybersecurity specialist*).

3. Principi generali di comportamento

Nell'espletamento delle proprie attività e funzioni, oltre a conoscere e rispettare i principi dettati dal Codice Etico, dal Sistema di Gestione della Sicurezza dell'Informazione ISO 27001, dal Sistema di gestione della continuità operativa ISO 22301 sulla continuità operativa e ripristino da disastro e da ogni *policy*/procedura operativa o normativa interna adottata dalla Società, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, è necessario:

a) fornire ai Destinatari un'adeguata informazione e un puntuale aggiornamento relativamente al corretto utilizzo delle risorse informatiche aziendali ed al rischio di commissione di reati informatici;
b) limitare l'accesso alle informazioni secondo il criterio del "*need to know*" (ossia ai soggetti che, in ragione delle funzioni svolte, ne abbiano necessità);
c) effettuare, nel rispetto della normativa sulla *privacy*, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
d) predisporre e mantenere adeguate difese fisiche a protezione dei server della Società e degli ulteriori sistemi informatici aziendali.

Inoltre, è assolutamente vietato:

a) scaricare file di immagini o video che non hanno uno scopo professionale, inviare catene di Sant'Antonio via e-mail, giocare, etc.
b) installare software su un device aziendale senza l'autorizzazione esplicita dell'IT Manager;
c) utilizzare applicazioni eseguibili e altro codice mobile, tranne quando preventivamente autorizzato;
d) utilizzare strumenti di crittografia (crittografia) su un device aziendale, tranne nei casi specificati nei criteri di classificazione delle informazioni;
e) scaricare il codice del programma da un supporto esterno;
f) divulgare informazioni relative ai sistemi informatici aziendali;
g) utilizzare i sistemi informatici aziendali per finalità non connesse alla funzione svolta o comunque contrarie al Modello e al Codice Etico;
h) introdurre in azienda e collegare alla rete aziendale computer, periferiche (es. chiavette USB, hard disk ecc.), altre apparecchiature o software senza la preventiva autorizzazione del Responsabile IT e, in qualunque modo, modificare la configurazione rilasciata dalla Funzione IT di postazioni di lavoro fisse o mobili;
i) porre in essere qualunque attività abusiva di intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche, nonché installare apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche;
j) installare software con licenze non valide (ciò anche a tutela della commissione di reati di cui all'art. 25 novies D. Lgs. 231/2001);
k) acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (quali ad esempio sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.);
l) ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti con metodi o procedure differenti da quelle a tale scopo autorizzate dalla Società;

m) divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti e terze parti;
n) manomettere, sottrarre o distruggere il patrimonio informatico aziendale, danneggiare o interrompere un sistema informatico o telematico di terzi, pubblici o privati, nonché diffondere apparecchiature, dispositivi o programmi informatici diretti a danneggiare od interrompere un sistema informatico o telematico di terzi, compresi archivi, dati e programmi;
o) distorcere, oscurare, sostituire la propria identità e inviare e-mail anonime o riportanti false generalità;
p) effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che ciò non sia esplicitamente previsto nei propri compiti lavorativi;
q) effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti col cliente (vulnerability test, penetration test) e previsto nei propri compiti lavorativi;
r) sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
s) comunicare a persone non autorizzate, interne o esterne all'azienda, i controlli implementati sui sistemi informatici e le modalità con cui sono utilizzati e/o rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
t) realizzare qualunque condotta finalizzata, in generale, alla duplicazione, di programmi per elaboratore protetti dal diritto d'autore o di banche-dati sulla memoria fissa del computer;
u) installare programmi per elaboratore non compresi tra quelli oggetto di accordo con il cliente;
v) costringere taluno, mediante accessi abusivi a sistemi informatici, intercettazioni e impedimenti e/o interruzione di comunicazioni telematiche, alterazione di comunicazioni informatiche, danneggiamento di dati, informazioni e sistemi informatici anche di pubblico interesse (o la minaccia di compiere tali atti), a porre in essere determinate condotte o omettere qualche cosa che possa comportare un profitto ingiusto per Axians, con altrui danno.

4. Protocolli specifici di comportamento

Ad integrazione ed ai fini di fornire un dettaglio operativo rispetto ai principi già declinati nel Codice Etico e nel presente Modello, nonché al fine di regolamentare la gestione dell'infrastruttura informatica e l'utilizzo dei sistemi informativi e telematici aziendali, AXIANS ha adottato le seguenti procedure:

- PR_03_Appendice 1 – Elenco dei requisiti legali

- PR_03_Procedura per identificazione dei requisiti
- PR_09.95_Procedura lavorare in aeree sicure
- PR_09.10.1_Procedura di business continuity e disaster recovery
- PR_09.20_Procedura incident management
- PR_12_Internal audit
- PR_14_Procedura per l'azione correttiva
- PR_15.01_Vulnerability Management
- RG_09.01_Regolamento dei sistemi informatici

Inoltre, sono state emanate le seguenti politiche:

- PO_05.01_Politica di capacity management
- PO_05_Politica sicurezza delle informazioni
- PO_06.03_Valutazione del rischio e metodologia di trattamento del rischio
- PO_09.02_Politica_Clear_Desk_e_Clear_Screen
- PO_09.03_Politica_Mobile Device e SmartWorking
- PO_09.04_Politica_Bring_your_own_device_BYOD
- PO_09.06_Politica_Classificazione delle informazioni
- PO_09.09_Politica gestione delle modifiche
- PO_09.10_Politica_Backup
- PO_09.12_Politica di smaltimento distruzione
- PO_09.14_Politica controllo degli accessi
- PO_09.16_Politica Sviluppo Sicuro
- PO_09.18_Politica Sicurezza dei Fornitori
- POLKPI_10_Metriche KPI

si prevedono i seguenti ulteriori protocolli specifici di comportamento:

A. Gestione e utilizzo dell'infrastruttura tecnologia e dei sistemi informatici e telematici aziendali
B. Gestione di software e banche dati

In conformità a quanto previsto dalle procedure aziendali e dalle *policy* di Gruppo richiamate:

- ogni utente deve essere identificato attraverso un codice identificativo che soddisfi i seguenti criteri di sicurezza:
  - deve essere personale e univoco;
  - non può essere assegnato ad altri utenti neppure in tempi diversi;
- le credenziali di accesso devono essere memorizzate sui sistemi informatici mediante opportuni meccanismi (es. cifratura) che consentano di garantire un adeguato livello di sicurezza;

- le utenze di default fornite dai produttori di sistemi hardware o software o da fornitori di applicativi, tools o soluzioni software, ove tecnicamente possibile, devono essere disabilitate, oppure le password devono essere cambiate al primo accesso con altre password di complessità e robustezza adeguate;
- le credenziali di accesso devono essere comunicate all'utente in forma strettamente confidenziale; suddividendo le comunicazioni tra invio del codice identificativo ed invio della componente segreta (quale ad esempio la password), eventualmente con mezzi di comunicazione diversi, quali cartaceo e telematico;
- la password relative ad utenze amministrative/privilegiate di sistema (es: administrator, root) deve essere custodita adeguatamente definita, si suggerisce almeno 15 caratteri, e protetta;
- la password di accesso relativa alle utenze di default fornite dai produttori di software e/o hardware, ove non sia stato tecnicamente possibile una loro disabilitazione, devono essere obbligatoriamente modificate in base alle regole sopra definite;
- devono essere disabilitate le utenze non utilizzate da almeno sei mesi;
- nel caso di interventi di manutenzione / assistenza / riparazione da parte di persone esterne, l'accesso ai sistemi informatici deve avere validità limitata;
- l'accesso ai sistemi deve avvenire attraverso un processo di: a) identificazione: per la verifica dell'esistenza e validità della user-id assegnata all'utente; b) autenticazione: per la verifica della correttezza della componente segreta (password, PIN…) fornita dall'utente;
- l'accesso ai sistemi sia dall'interno della rete sia da remoto deve avvenire mediante protocolli di comunicazione sicuri (Segregation Of Duties all'interno e inoltre dall'esterno, HTTPS, VPN o equivalente);
- l'accesso ai sistemi deve avvenire unicamente tramite utenze nominali e non tramite utenze condivise / di gruppo;
- unicamente nei casi in cui non risulti tecnicamente possibile effettuare le medesime attività mediante utenze nominali si potrà ricorrere ad utenze di amministrazione generiche (es. Administrator, root, etc.);
- deve essere gestita la storicizzazione delle utenze al fine di garantire la corretta ricostruzione dei dati degli utenti;
- devono essere definite delle procedure per consentire l'accesso ai dati in tutti i casi in cui la prolungata assenza o impedimento della persona renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza;
- la profilazione dei diritti di accesso alle informazioni ed alle risorse deve basarsi sui principi di: a) need to know b) least privilege c) segregation of duties;
- l'accesso remoto dei dipendenti e terze parti alle reti ed ai sistemi aziendali deve essere preventivamente autorizzato e concesso unicamente agli utenti che abbiano effettive esigenze lavorative in tal senso;
- al fine di gestire adeguatamente le utenze, periodicamente devono essere attuate procedure di verifica del corretto utilizzo dei privilegi ad esse assegnate, in ottica sia di conformità alla normativa vigente in materia di sicurezza e protezione dei dati personali (Regolamento Europeo 2016/679) sia delle norme ISO 27001;

- il rispetto delle misure per la salvaguardia di dati, programmi e sistemi informatici deve essere periodicamente verificato a cura dell'Amministratore di sistema;
- deve essere redatto e mantenuto aggiornato un elenco dei *software* installati con riferimento ai relativi strumenti elettronici, fornendo evidenza del possesso delle licenze utilizzate;

- sono chiaramente individuati i responsabili dell'installazione di *software*; l'installazione di software deve avvenire previo riscontro della licenza e previa autorizzazione della funzione IT; l'installazione deve inoltre essere tempestivamente registrata nell'elenco di cui sopra;
- le attività svolte da parte di fornitori terzi (*networking*, gestione software applicativi e sistemi *hardware*, ecc.) devono rispettare i principi e le regole aziendali al fine di tutelare la sicurezza dei dati ed il corretto accesso da parte dei soggetti ai sistemi applicativi ed informatici (come specificato anche nell'ambito del Sistema di Sicurezza delle Informazioni e *Data Protection*);
- l'accesso ai sistemi di registrazione contabile è consentito ai soli addetti delle funzioni di contabilità e amministrazione;
- è consentito l'accesso ad Internet, mediante il normale software di navigazione in rete in dotazione, solo se effettuato per scopi leciti e tali da non pregiudicare il patrimonio informativo aziendale;
- non deve essere consentito l'accesso alle aree riservate (quali *server rooms*, locali tecnici, ecc.) alle persone che non dispongono di idonea autorizzazione, temporanea o permanente e, in ogni caso, nel rispetto della normativa (interna ed esterna) vigente in materia di tutela dei dati personali.

La Società è inoltre soggetta alla Direttiva NIS2 (Direttiva UE 2022/2555 del Parlamento Europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione Europea).
La normativa impone ai soggetti destinatari — tra cui rientra la Società — obblighi in materia di:
- adozione di misure tecniche e organizzative di gestione del rischio informatico;
- notifica degli incidenti significativi alle autorità competenti;
- adempimenti registrativi nei confronti di ACN.

In tale contesto, la Società ha avviato un percorso strutturato di adeguamento agli obblighi previsti dalla normativa entro i termini stabiliti dalla Legge.

Nell'ambito degli adempimenti previsti dalla normativa NIS2, la società ha:

a. indicato sia il punto di contatto, il responsabile del sistema di gestione e della sicurezza delle informazioni e il suo sostituto;
b. è stata individuata come soggetto essenziale per l'anno 2026;
c. indicato anche il referente csirt e il relativo sostituto;
d. effettuato l'identificazione dei fornitori;
e. inserito la procedura di Vulnerability Management (PR_15.01);
f. inserito la Procedura Incident Management (PR_09.20);
g. ottenuto la certificazione ISO/IEC 27035 sulla gestione degli incidenti di sicurezza informatica.

Axians, nel rispetto del Decreto legislativo n. 160 del 9 settembre 2026, utilizza l'AI in modalità sicura e sulla base delle linee guida di gruppo.
Lo strumento d'Intelligenza Artificiale utilizzato è Copilot web, una soluzione sicura che tutela la riservatezza, la disponibilità e l'integrità delle informazioni. Copilot offre assistenza nella redazione di testi, nel recupero di informazioni e nella generazione di codici. Ai clienti viene fornita una funzionalità AI per la previsione dei consumi energetici all'interno di XSONA Energy e XSONA Analytics, piattaforma IoT e una chatbot integrato di nome Aura. Per quanto riguarda l'AI di terze parti vengono utilizzati modelli Microsoft Azure OpenAI (GPT-5.4, GPT-5.4-mini, text-embedding-3-

small), usati tramite API.
I modelli non vengono addestrati né personalizzati (nessun fine-tuning) e i dati dei clienti non vengono usati per l'addestramento. Nei servizi forniti ai clienti è incorporata come AI: PaloAlto XSIAM e TrendAI VisionOne.
La società sta comunque implementando una policy interna in materia di utilizzo dell'intelligenza artificiale.

In conformità a quanto previsto dal regolamento dei sistemi informatici occorre:

- utilizzare strumenti di IA approvati dall'azienda, nella specie Copilot, oppure anonimizzare le informazioni prima di caricarle;
- in caso si utilizzino strumenti di Al diversi da Copilot, verificare sempre che le informazioni condivise con sistemi di IA siano non sensibili;
- seguire il principio di minimizzazione dei dati: condividere solo ciò che è strettamente necessario;
- controllare l'accuratezza dei contenuti generati (l'IA può produrre errori o informazioni inventate).

Occorre poi evitare di:

- inserire nelle piattaforme di IA diverse da Copilot: dati personali di clienti, colleghi o terzi; documenti aziendali riservati; informazioni strategiche, finanziarie o protette da copyright.
- utilizzare strumenti di IA privi di adeguate garanzie di sicurezza;
- Affidarsi alla risposta dell'IA senza una verifica umana;
- generare o diffondere deepfake senza autorizzazione;
- utilizzare immagini, voci o video alterati mediante AI senza autorizzazione o comunque senza esplicitare con la dicitura "immagine generata con intelligenza artificiale".

È vietato dall'organizzazione l'utilizzo di altri tool, che non garantiscono la sicurezza necessaria, ed esporrebbero Axians a un elevato rischio di violazione dei dati.

5. Reporting all'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di verificare la corretta applicazione dei protocolli di cui alla presente Parte Speciale, i Responsabili delle Funzioni coinvolte nella gestione dei processi sensibili di cui al punto 2) dovranno trasmettere all'OdV le informazioni e le segnalazioni previste dalle procedure "*PMOG02 ODV Procedura Flussi informativi*" e "*PMOG01 Procedura Segnalazione Violazioni Whistleblowing*".

Parte Speciale 5

Corruzione tra privati

La presente Parte Speciale trova applicazione per i reati di cui agli articoli 2635 comma 3 e 2635-bis comma 1 c.c., introdotti tra i reati societari ex art. 25-ter del Decreto, come dettagliatamente definiti nell'**Allegato A**.

1. I delitti di corruzione tra privati e istigazione alla corruzione tra privati

Il delitto di corruzione tra privati di cui all'art. 2635 c.c. è stato introdotto nel catalogo dei reati presupposto ad opera della legge n. 190/2012, in sostituzione della fattispecie di "infedeltà a seguito di dazione o promessa di utilità".
Successivamente, il D. Lgs. n. 38/2017 ne ha esteso la portata applicativa ed ha, altresì, introdotto tra le fattispecie rilevanti ai sensi del Decreto il reato di istigazione alla corruzione tra privati (art. 2635-bis c.c.), prevedendo l'applicabilità ad entrambe le fattispecie delle sanzioni interdittive, in aggiunta alle sanzioni pecuniarie già previste.
Infine, la Legge n. 3/2019 ha modificato il regime di procedibilità dei predetti reati introducendo la procedibilità d'ufficio.

In considerazione della mappatura dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati:

- corruzione tra privati (art. 2635, comma 3, c.c.);
- istigazione alla corruzione tra private (art. 2635 bis, comma 1 c.c.).

Per una disamina approfondita dei reati e delle sanzioni applicabili all'ente si rimanda all'**Allegato A**.

2. Attività sensibili

In relazione alle fattispecie di corruzione e istigazione alla corruzione tra privati, si ritengono maggiormente a rischio i seguenti processi:

A) gestione commesse e rapporti con i clienti;
B) gestione processo di ricerca, selezione, assunzione e gestione del personale;
C) gestione note spese e spese di rappresentanza;
D) gestione dei crediti;
E) gestione dei rapporti con terze parti (fornitori, consulenti, appaltatori, agenti, ecc.)
F) concessione di omaggi, liberalità e sponsorizzazioni.

3. Principi generali di comportamento

Nell'espletamento delle proprie attività e funzioni, oltre a conoscere e rispettare i principi dettati dal Codice Etico, dal Codice di Condotta Anticorruzione, da ogni *policy* di Gruppo e procedura operativa o normativa interna adottata dalla Società, i Destinatari dovranno rispettare le regole di comportamento di seguito definite.

E' fatto divieto di:

a) offrire o promettere denaro o altre utilità, di qualsiasi natura, anche per interposta persona, a clienti o potenziali tali al fine di far ottenere un qualsiasi vantaggio alla Società;
b) porre in essere qualsiasi attività in grado di generare conflitto di interessi con società o enti terzi, funzionale alla commissione di un reato di cui alla presente sezione;
c) compiere qualsiasi operazione volta alla creazione di fondi extracontabili.

Inoltre:

d) tutto il personale che ha gerarchicamente poteri direttivi e quindi di controllo e vigilanza sui dipendenti che si interfacciano son soggetti terzi (es. clienti, partner, concorrenti) deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali violazioni del Modello o situazioni di irregolarità rilevanti ai fini del Decreto;
e) i dipendenti della Società che effettuano pagamenti o, in generale, transazioni con terze parti, devono prendere conoscenza dei principi di comportamento e dei protocolli adottati dalla Società per fronteggiare i tentativi di corruzione.

4. Protocolli specifici di comportamento

Ad integrazione delle norme di comportamento di cui sopra ed al fine di fornire un dettaglio operativo rispetto ai principi già declinati nel Codice Etico, nel Codice di Condotta Anticorruzione e nelle *policy* di Gruppo, la Società ha formalizzato le specifiche procedure e istruzioni operative aventi ad oggetto i processi a rischio identificati:

- PRO01_Bidding Procedure;
- IOP03_Gestione approvazione Pricesheet;
- PRO02_Gestione commesse;
- PMOG03_ Gestione Omaggi & Inviti;
- VEI_ Guidelines Omaggi e Inviti BU_Level;
- PURU01_Gestione della ricerca e della selezione del personale;
- PDSG11_Gestione Trasferte Estero;
- PURU10_Travel Policy;
- PURU03 Procedura Gestione e Sviluppo delle Risorse;
- PRO11_Pre sales procedure;
- PRO13_Gestione degli Acquisti;
- PRO15_Qualificazione e Valutazione fornitori;
- PRO16_Gestione dei rapporti consulenziali.

In aggiunta ai principi di cui sopra, si prevedono i seguenti protocolli specifici di comportamento:

A. Gestione commesse e rapporti con i clienti

Nella gestione degli ordini di vendita e, in particolare, nella fase di negoziazione con il cliente, tutti i Destinatari del Modello che, a vario titolo, partecipino alla gestione di tale attività, sono tenuti ad osservare il Codice Etico, il Codice di Condotta Anticorruzione, nonché le *policy* di Gruppo e le procedure interne adottate dalla Società. Inoltre, si applicano a tali soggetti le seguenti regole di comportamento:

- prima di concludere un contratto o un ordine, occorre provvedere alla verifica dell'affidabilità della controparte, mediante gli opportuni controlli; nessuna offerta commerciale può essere finalizzata in assenza della necessaria approvazione; in particolare, l'opportunità commerciale deve essere validata dalla funzione competente in relazione al valore della commessa e alla BU di appartenenza, secondo i livelli approvativi definiti dalla procedura "*PRO01 Bidding Procedure*";
- alla definizione dell'offerta commerciale devono concorrere una pluralità di funzioni; in particolare, l'Area Sales e/o Pre-Sales, in base alla tipologia di offerta, predispone un documento (*pricesheet*) di stima dei costi necessari alla realizzazione dello specifico progetto (es. fornitura, manodopera, ecc.); detto documento è poi approvato dalle funzioni competenti in base agli scaglioni di valori definiti nella procedura "*IOP03 Gestione approvazione Pricesheet*";
- la Società ha implementato un listino prezzi (*file Excel*) sia per le attività a progetto che per le offerte semplici; eventuali deroghe ai prezzi di listino sono gestite attraverso la procedura "*IOP03 Gestione approvazione Pricesheet*";
- la negoziazione con il cliente è gestita dalla funzione commerciale con l'eventuale coinvolgimento del *Legal Counsel* per l'elaborazione, revisione o negoziazione delle condizioni generali di contratto (**CGC**);
- deve essere garantita la tracciabilità dei prezzi applicati, di eventuali sconti o promozioni concordate, nonché di eventuali variazioni dell'offerta;
- in caso di modifiche dell'offerta commerciale, l'area commerciale deve aggiornare le voci del pricesheet (costi, utili, ecc.) e ottenere nuovamente l'approvazione deldocumento da parte delle funzioni responsabili, secondo l'iter previsto per la commessa principale; detta approvazione è rilasciata dal soggetto competente in base al valore complessivo della commessa. Il *Customer Care* verifica che l'approvazione sia stata rilasciata e provvede all'aggiornamento della commessa nel gestionale aziendale: la nuova offerta viene registrata come "revisione" dell'offerta iniziale o modifica d'ordine;
- l'approvazione di cui sopra è evidenziata dalla validazione digitale del *pricesheet* attraverso la piattaforma CRM (*Salesforce*);
- la documentazione a corredo dell'offerta (es. evidenza dell'accettazione dell'offerta/ordine/contratto, pricesheet ecc.) è archiviata sul *file server* aziendale/*sharepoint* della BU specifica; la documentazione è verificata dal *Customer Care*.
- è responsabilità del *Customer Care* verificare che (i) il cliente non risulti bloccato per insoluti, (ii) i dati siano corretti e completi, (iii) sia presente la conferma/firma scritta del cliente
- il Sales/Pre-Sales verifica che l'ordine/contratto corrisponda all'offerta.
- le provvigioni eventualmente spettanti dall'agente sono verificate anch'esse a cura del

Customer Care, che ne accerta la corrispondenza a quanto pattuito nel contratto di agenzia. Eventuali eccezioni rispetto al contratto di agenzia devono essere autorizzate dall'Amministratore Delegato o dal diverso soggetto munito dei necessari poteri (es. *BU Manager*).

B. Gestione processo di ricerca, selezione, assunzione e gestione del personale
C. Gestione note spese e spese di rappresentanza
D. Gestione dei crediti
E. Gestione dei rapporti con terze parti (fornitori, consulenti, appaltatori, agenti, ecc.)

Con riferimento a tali processi sensibili, si applicano, per analogia, i protocolli previsti nella **Parte Speciale 1**, in quanto compatibili. Per il paragrafo B. si applicano i paragrafi F., G. e H. della parte speciale 1. Per il paragrafo C. si applica il paragrafo F. della parte speciale 1. Per il paragrafo D. si applica il paragrafo E. della parte speciale. Per il paragrafo E. si applica il paragrafo C. e D. della parte speciale.

F. Concessione di omaggi, liberalità e sponsorizzazioni

In conformità alla procedura "**PMOG03_Gestione Omaggi&Inviti"**

- è vietato corrispondere omaggi a familiari o amici propri o di terzi, salvo vi sia l'esigenza di alcune circostanze particolari (ad esempio, celebrazione di un evento significativo nello svolgimento di un progetto) e, in ogni caso, previa autorizzazione del *BU Manager*;
- sono vietati se offerti a società di *rating* o a società di certificazione (e ai loro dipendenti amministratori, collaboratori ecc.) al fine dell'ottenimento di giudizi favorevoli;
- le sponsorizzazioni possono riguardare eventi ed iniziative a carattere sociale, culturale, sportivo ed artistico; studi, ricerche, convegni e seminari di rilevanza sociale e di interesse per la Società;
- i pranzi e le cene con terze parti dovranno trattare di questioni di natura professionale e la relativa spesa dovrà essere di modico valore, coerentemente con gli usi locali;
- non possono essere estesi inviti a pranzi/cene a soggetti non direttamente correlati all'attività professionale svolta.

Si applicano, inoltre, i protocolli di cui alla **Parte Speciale 1**.

5. Reporting all'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di verificare la corretta applicazione dei protocolli di cui alla presente Parte Speciale, i Responsabili delle Funzioni coinvolte nella gestione dei processi sensibili di cui al punto 2) dovranno trasmettere all'OdV le informazioni e le segnalazioni previste dalle procedure "*PMOG02 ODV Procedura Flussi informativi*" e "*PMOG01 Procedura Segnalazione Violazioni Whistleblowing*".

Parte Speciale 6

Delitti di criminalità organizzata, transnazionali e di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria

La presente Parte Speciale si riferisce ai reati di cui agli articoli 24-ter e 25-decies del Decreto e all'art. 10, L. 146/2006, come dettagliatamente definiti nell'**Allegato A**.

1. Reati di criminalità organizzata, reati transnazionali e delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (artt. 24-ter, 25-decies del D. Lgs. 231/2001 e art. 10 della L. 146/2006)

La Legge 15 luglio 2009 n. 94, recante disposizioni in materia di sicurezza pubblica, ha previsto l'inserimento nel Decreto dell'articolo 24-ter relativo ai "Delitti di Criminalità Organizzata".
Con riferimento a tale categoria di reati presupposto, in considerazione della mappatura dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati:

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso (art. 416 bis c.p.);
- Scambio elettorale politico-mafioso (art. 416 ter c.p.);
- tutti i delitti commessi avvalendosi delle condizioni previste dall'art. 416-bis c.p. per agevolare l'attività delle associazioni previste dallo stesso articolo (L. 203/91).

Occorre altresì considerare che la Legge 16 marzo 2006 n. 146 (Legge 146/06) ha introdotto tra i reati rilevanti ai sensi del Decreto la nuova categoria dei "reati transnazionali". Finalità della citata Legge è quella di fornire più efficaci mezzi di prevenzione e repressione in relazione ad organizzazioni criminali che agiscono a livello internazionale, per il cui contrasto si rende necessaria la collaborazione tra diversi Stati.
Ai sensi dell'art. 3 della Legge 146/06, si considera transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato e il fatto:

- sia commesso in più di uno Stati;
- ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
- ovvero sia commesso in uno Stato, ma nello stesso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato, ovvero;
- sia commesso in uno Stato, ma abbia effetti sostanziali in un altro Stato.

L'articolo 10 della Legge 146/06 elenca le fattispecie penali la cui commissione determina la responsabilità amministrativa dell'Ente, nel caso in cui sussistano i sopra illustrati elementi costitutivi del reato transnazionale e siano, naturalmente, ravvisabili i criteri di imputazione di responsabilità all'Ente medesimo previsti dal Decreto (*infra*, **Premessa, Parte Generale**).
I reati transnazionali ritenuti astrattamente applicabili alla Società, oltre a quelli di cui agli artt. 416, 416 bis c.p., sono i seguenti:

- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.);
- favoreggiamento personale (art. 378 c.p.).

In relazione all'attività svolta dalla Società, infatti, si ritiene che possa ragionevolmente escludersi l'applicabilità dei reati concernenti l'immigrazione clandestina, il contrabbando di tabacchi lavorati esteri, nonché il delitto di associazione finalizzata al traffico di sostanze stupefacenti o psicotrope.

Il delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria di cui all'art. 25-decies del D. Lgs. 231/2001, invece, potrebbe manifestarsi qualora la Società, con violenza o minaccia o con offerta o promessa di danaro o di altra utilità, inducesse la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale, a non rendere dichiarazioni o a rendere dichiarazioni mendaci (che abbia la facoltà di non rendere).

Si precisa che l'introduzione di alcuni reati nella presente Parte Speciale ha carattere meramente prudenziale in quanto, pur non sussistendo elementi specifici da cui dedurre l'esistenza di attuali rischi, si tratta di reati sui quali la Società intende comunque mantenere un livello alto di attenzione.

Per una disamina più approfondita di tali Reati Presupposto e delle relative sanzioni, si rinvia all'**Allegato A**.

2. Attività sensibili

In relazione alle fattispecie richiamate nella presente Sezione di Parte Speciale, si ritengono maggiormente a rischio i seguenti processi:

A) selezione, assunzione e gestione del personale;
B) gestione delle transazioni con terze parti (es. fornitori, appaltatori, agenti, clienti, ecc.);
C) gestione dei flussi finanziari;
D) rapporti con soggetti coinvolti in procedimenti giudiziari.

3. Principi generali di comportamento

Le disposizioni della presente Parte Speciale si applicano a tutti i Destinatari del presente Modello che, a qualunque titolo e per conto o nell'interesse di AXIANS, intrattengano rapporti con soggetti coinvolti in procedimenti giudiziari (civili, amministrativi e penali), agli incaricati della gestione dei flussi finanziari (incassi e pagamenti da e verso terzi), ai soggetti coinvolti nel processo di *recruiting*, nonché a tutti coloro che intrattengano rapporti economici e contrattuali con Società (consulenti, fornitori, partner commerciali, ecc.), in forza di apposite clausole contrattuali.

In via generale, a tali soggetti è richiesto di:

a) evadere con tempestività, correttezza e buona fede tutte le richieste provenienti dagli organi di polizia giudiziaria e dall'autorità giudiziaria inquirente e giudicante, fornendo tutte le informazioni, i dati e le notizie eventualmente utili;
b) mantenere, nei confronti degli organi di polizia giudiziaria e dell'autorità giudiziaria un comportamento disponibile e collaborativo in qualsiasi situazione;
c) informare tempestivamente l'Organismo di Vigilanza in merito a comportamenti non conformi alle regole della presente sezione.

È fatto divieto di:

d) porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, considerati individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra citate (art. 24-ter e 25-decies del Decreto e reati transnazionali);
e) promuovere, costituire, dirigere, organizzare, finanziare, partecipare ad associazioni di cui agli artt. 416 e 416-bis c.p., nonché intrattenere relazioni con soggetti di cui sia nota o sospettata l'appartenenza alle associazioni medesime;
f) effettuare prestazioni in favore di fornitori, consulenti e partner in generale che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito o in relazione al tipo di incarico da svolgere;
g) indurre i soggetti chiamati a rendere dichiarazioni davanti all'Autorità Giudiziaria, a non rendere dichiarazioni o a rendere dichiarazioni mendaci.

4. Protocolli specifici di comportamento

Ad integrazione ed ai fini di fornire un dettaglio operativo rispetto ai principi già declinati nel Codice Etico e nel presente Modello, AXIANS ha adottato le seguenti procedure:

- PURU01_Gestione della ricerca e selezione del personale;
- PURU03_Gestione e sviluppo delle risorse umane;

- PMOG05_Procedura Gestione Flussi Finanziari ed Economici;
- PMOG03_Gestione Omaggi & Inviti;
- VEI_ Guidelines Omaggi e Inviti BU_Level;
- PRO15_Qualificazione e Valutazione fornitori;
- PRO13_Gestione degli Acquisti.

In aggiunta a tali presidi di controllo, si predono i seguenti ulteriori protocolli specifici di comportamento:

A. Selezione, assunzione e gestione del personale
B Gestione dei flussi finanziari

Si osservano, in quanto compatibili, le disposizioni di cui alla **Parte Speciale 1**.

C. Gestione delle transazioni con terze parti (es. fornitori, appaltatori, agenti, clienti, ecc.)

Con riferimento a tale processo, in aggiunta ai protocolli previsti alla **Parte Speciale 1**, i Destinatari devono:

- accertarsi che i terzi con cui intrattengono rapporti non abbiano sede o collegamenti con Paesi considerati come non cooperativi dal Gruppo Azione Finanziaria contro il riciclaggio di denaro (GAFI).
- verificare l'effettivo adempimento della prestazione oggetto del rapporto contrattuale;
- assicurare la corretta archiviazione di tutta la documentazione prodotta nell'ambito del processo tramite sistema gestionale informatico, in modo da lasciare evidenza sia delle diverse fasi del processo di selezione del fornitore che della verifica dell'effettivo adempimento della prestazione;
- liquidare i compensi in modo trasparente, sempre documentabile e ricostruibile ex post.

D. Rapporti con soggetti coinvolti in procedimenti giudiziari

È fatto divieto a tutti i Destinatari del Modello di:

- intrattenere rapporti con persone sottoposte alle indagini preliminari e imputati in un processo penale al fine di turbare la loro libertà di autodeterminazione;
- riconoscere denaro, forme di liberalità o altre utilità a dipendenti o terzi che siano sottoposti a indagini preliminari e/o imputati in un processo penale, per indurli a omettere dichiarazioni o a falsare le stesse in favore di AXIANS;
- aiutare taluno – anche se non imputabile e/o se risulta non aver commesso reato – ad eludere le investigazioni delle autorità pubbliche, comprese quelle svolte da organi della Corte penale internazionale, o a sottrarsi alle ricerche effettuate dai medesimi soggetti.

5. Reporting all'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di verificare la corretta applicazione dei protocolli di cui alla presente Parte Speciale, i Responsabili delle Funzioni coinvolte nella gestione dei processi sensibili di cui al punto 2) dovranno trasmettere all'OdV le informazioni e le segnalazioni previste dalle procedure "*PMOG02 ODV Procedura Flussi informativi*" e "*PMOG01 Procedura Segnalazione Violazioni Whistleblowing*".

Parte Speciale 7

Reati contro l'industria e il commercio e in materia di falsità

La presente Parte Speciale si riferisce ai reati di cui agli artt. 25-bis e 25-bis.1 del Decreto, come dettagliatamente definiti nell'**Allegato A**.

1. Le fattispecie contro l'industria e il commercio e in materia di falsità in monete, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento (artt. 25-bis.1 e 25-bis del D. Lgs. 231/2001)

In considerazione della mappatura dei rischi effettuata, i delitti contro l'industria e il commercio ex art. 25-bis.1 del D. Lgs. 231/2001 ritenuti astrattamente applicabili alla struttura societaria di AXIANS sono i seguenti:

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.).

Per analogia, vengono ricompresi nella presente sezione di Parte Speciale anche i reati in materia di falsità, previsti dall'art. 25-bis del D. Lgs. 231/2001. Relativamente a tale categoria di Reati Presupposto, sono risultati potenzialmente realizzabili le seguenti fattispecie:

- Contraffazione, alterazione o uso di marchi o di segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello stato e commercio di prodotti con segni falsi (art. 474 c.p.).

Per una disamina più approfondita di tali Reati Presupposto e delle relative sanzioni, si rinvia all'**Allegato A**.

2. Attività sensibili

In relazione alle fattispecie richiamate nella presente Sezione di Parte Speciale, si ritengono maggiormente a rischio i seguenti processi:

A) gestione vendite e *marketing* (commercializzazione e promozione di prodotti attraverso tutti i canali di vendita);

B) installazione, aggiornamento, gestione e manutenzione di dispositivi e/o sistemi informatici e/o informativi, sia aziendali che presso la clientela;
C) rapporti con i Terzi (clienti, fornitori ecc.).

3. Principi generali di comportamento

AXIANS riconosce i diritti di proprietà intellettuale ed industriale e si impegna ad agire nel pieno rispetto degli stessi, nonché in conformità alle disposizioni di legge che li tutelano.
Pertanto, tutti i Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività sensibili rispetto ai reati in materia di falsità in strumenti o segni di riconoscimento di cui all'art. 25-bis del D.Lgs. 231/2001 sono tenuti ad osservare, oltre al Codice Etico, alle *policy* di Gruppo e a tutte le procedure e le norme interne che regolamentano tali attività, i principi di comportamento di seguito elencati.
In via generale, a tali soggetti è richiesto di:

a) rispettare i principi etici volti a stigmatizzare qualsiasi comportamento contrario alle corrette pratiche concorrenziali presenti nel Codice Etico e nelle policy di Gruppo;
b) partecipare alle iniziative formative periodiche nei confronti dei soggetti responsabili delle aree maggiormente coinvolte sugli aspetti competitivi (i.e. direzione, area commerciale, area marketing) riguardo alle problematiche afferenti agli aspetti di concorrenza sleale;
c) mantenere un comportamento corretto e trasparente con i clienti in merito alle caratteristiche dei prodotti impiegati; in particolare, è necessario fornire informazioni veritiere, precise ed esaurienti circa la quantità e qualità dei prodotti venduti;
d) svolgere le attività di sviluppo e ricerca di nuovi segni distintivi e/o di qualsivoglia bene qualificabile come opera dell'ingegno ai sensi di legge, nel rispetto del valore della legalità e in attuazione delle norme interne, comunitarie e internazionali poste a tutela della proprietà industriale;
e) verificare quale sia il legittimo titolare di ciascuna opera dell'ingegno (in particolare: testi, musiche, immagini, disegni, ecc.), marchio e/o altro segno distintivo, brevetto, informazione riservata e/o qualsivoglia altro bene tutelato dalla normativa di settore, eventualmente impiegato dal Destinatario nello svolgimento della propria attività lavorativa;
f) acquisire previamente i necessari diritti di p.i. dal legittimo titolare dei beni sopracitati; a tal fine, nei contratti conclusi con detti titolari, la Società avrà cura di inserire apposite dichiarazioni sostitutive attestanti la titolarità dei diritti in capo al dichiarante, inserendo apposite manleve in favore di AXIANS qualora le dichiarazioni non risultino veritiere;
g) informare tempestivamente l'Organismo di Vigilanza di qualsivoglia comportamento anomalo, o comunque non conforme alle disposizioni della presente sezione, anche da parte di fornitori esterni alla Società.

4. Protocolli specifici di comportamento

In aggiunta ai principi di cui sopra, si prevedono i seguenti protocolli specifici di comportamento:

A. Gestione vendite e *marketing* (commercializzazione e promozione di prodotti attraverso tutti i canali di vendita)

Nella gestione dell'attività di vendita e *marketing*, tutti i Destinatari del presente Modello devono:

- rispettare le norme in materia di proprietà intellettuale, attraverso il controllo dei mezzi di comunicazione aziendali, dei sistemi informatici (anche grazie all'uso di filtri, *firewall*, controllo dei livelli di traffico, controllo dei procedimenti di *file sharing*), al fine di impedire l'impiego di beni aziendali per adottare condotte che violino la tutela dei diritti d'autore;
- astenersi dal riprodurre o diffondere, in qualunque forma e senza diritto, l'opera intellettuale altrui, in mancanza di accordi contrattuali formalizzati per iscritto con i relativi titolari per il relativo sfruttamento economico o in violazione dei termini e delle condizioni previste in detti accordi.

Inoltre, è fatto divieto di:

- mettere in vendita o altrimenti in circolazione prodotti le cui qualità e caratteristiche siano diverse, anche solo parzialmente, da quelle dichiarate o pattuite;
- proporre alla clientela modelli, disegni ornamentali o opere dell'ingegno altrui;
- dichiarare caratteristiche del prodotto non veritiere o diverse da quelle effettive.

B. Installazione, aggiornamento, gestione e manutenzione di dispositivi e/o sistemi informatici e/o informativi, sia aziendali che presso la clientela

In base alle *policy* di Gruppo e alle procedure di AXIANS:

- è fatto divieto di installare presso la clientela prodotti per i quali le circostanze del caso concreto rendano evidente trattarsi di contraffazioni degli originali;
- l'installazione di programmi, che non siano già stati acquisiti a livello centralizzato, deve essere autorizzata dal Reparto IT;
- è possibile solo installare programmi informatici – sia internamente che presso terzi – solo dopo avere verificato la sussistenza e la validità della relativa licenza;
- in caso di condivisione di file (cd. *file sharing*), occorre accertarsi che tale condivisione e/o scambio avvenga in conformità alla normativa sul diritto d'autore e, comunque, all'interno degli ordinari e leciti circuiti commerciali dei beni oggetto di proprietà intellettuale;
- i medesimi controlli sono necessari anche per l'upload e il download di software, file e contenuti in genere, quando gli stessi siano protetti dal diritto d'autore.

Rapporti con i Terzi (clienti, fornitori ecc.)

Nei rapporti commerciali e contrattuali con terze parti (clienti, fornitori, ecc.), è necessario:

- ove ritenuto opportuno in relazione all'oggetto del contratto, inserire nel contratto clausole specifiche di manleva riferite all'osservanza delle norme in materia di proprietà intellettuale;
- verificare, anche confrontandone i prezzi con quelli ufficiali di listino del singolo fornitore, che la merce recapitata dai fornitori della Società (e, in special modo, la merce successivamente destinata ad essere installata presso i clienti della Società) provenga da soggetti autorizzati, e

non costituisca contraffazione di prodotti di terzi;

- prevedere, tramite apposite clausole contrattuali, l'impegno del fornitore – corredato da apposita manleva – a garantire l'originalità dei prodotti forniti alla Società;
- rispettare scrupolosamente il contenuto dei contratti stipulati con terzi aventi ad oggetto l'esercizio di diritti di proprietà intellettuale.

Si applicano, in quanto compatibili, i protocolli specifici di comportamento previsti dalla **Sezione 4** di Parte Speciale.

5. Reporting all'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di verificare la corretta applicazione dei protocolli di cui alla presente Parte Speciale, i Responsabili delle Funzioni coinvolte nella gestione dei processi sensibili di cui al punto 2) dovranno trasmettere all'OdV le informazioni e le segnalazioni previste dalle procedure "*PMOG02 ODV Procedura Flussi informativi*" e "*PMOG01 Procedura Segnalazione Violazioni Whistleblowing*".

Parte Speciale 8

Reati di ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita

La presente Parte Speciale si riferisce ai reati di cui all'art. 25-octies del Decreto, come dettagliatamente definiti nell'**Allegato A**.

1. Le fattispecie di riciclaggio, autoriciclaggio, reimpiego (art. 25-octies del D. Lgs. 231/2001)

In considerazione della mappatura dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati:

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648-ter 1c.p.).

Per una disamina più approfondita di tali Reati Presupposto e delle relative sanzioni, si rinvia all'**Allegato A**.

2. Attività sensibili

In relazione alle fattispecie di cui all'art. 25-octies del Decreto, si ritengono maggiormente a rischio i seguenti processi:

A) gestione dei rapporti con terze parti (es. fornitori, clienti, consulenti e partner);
B) gestione dei flussi finanziari.

3. Principi generali di comportamento

Nell'espletamento delle proprie attività e funzioni, oltre a conoscere e rispettare i principi dettati dal Codice Etico, da ogni *policy* di Gruppo e procedura operativa o normativa interna adottata dalla Società, i Destinatari dovranno rispettare le seguenti regole di comportamento.
In via generale, è richiesto ai Destinatari di:

a) utilizzare esclusivamente il sistema bancario per effettuare le transazioni monetarie/finanziarie così come richiesto dalla normativa, al fine di garantire la tracciabilità dei flussi finanziari;
b) selezionare i fornitori secondo criteri predefiniti di trasparenza, qualità ed economicità;
c) verificare periodicamente l'allineamento delle condizioni applicate con i fornitori e partner in affari (commerciali e finanziari) alle condizioni di mercato;

d) prestare particolare attenzione ai pagamenti ricevuti da istituti di credito/clienti esteri;
e) segnalare all'OdV eventuali rapporti contrattuali con clienti o terze parti che abbiano sede o residenza ovvero qualsiasi collegamento con Paesi considerati come non cooperativi dal GAFI ed eventuali anomalie nei pagamenti ricevuti.

È fatto altresì espresso divieto ai Destinatari di:

f) trasferire a qualsiasi titolo, se non per il tramite di banche o istituti di moneta elettronica o Poste Italiane S.p.A., denaro contante o libretti di deposito bancari o postali al portatore o titoli al portatore in euro o in valuta estera, quando il valore dell'operazione, anche frazionata, sia complessivamente pari o superiore al valore limite previsto dalla vigente normativa;
g) emettere assegni bancari e postali per importi superiori a quelli previsti dalla normativa vigente e che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
h) effettuare versamenti su conti correnti cifrati;
i) effettuare pagamenti su conti correnti di banche operanti in paesi ricompresi nelle liste "*tax heaven*" e in favore di società "*off-shore*";
j) compiere qualsiasi operazione volta alla creazione di fondi extracontabili.

4. Protocolli specifici di comportamento

Ad integrazione ed ai fini di fornire un dettaglio operativo rispetto ai principi già declinati nel Codice Etico e nel presente Modello, in relazione ai reati contemplati nella presente Sezione di Parte Speciale, AXIANS ha adottato le seguenti procedure:

- PMOG05_Procedura Gestione Flussi Finanziari ed Economici

Si prevedono, inoltre, i seguenti protocolli specifici di comportamento:

A. Gestione dei rapporti con terze parti (es. fornitori, clienti, consulenti e partner);

Tutti i Destinatari del presente Modello che, in ragione dell'incarico svolto, intrattegano rapporti con terze parti, devono:

- raccogliere e censire le informazioni più significative relative a clienti e fornitori (quali, a titolo puramente esemplificativo, il legale rappresentante, la nazione di residenza, il tipo di attività economica, i bilanci societari, la sede legale della Società, gli istituiti di credito utilizzati, coincidenza tra soggetto cui l'ordine è intestato e quello che incassa le relative somme ecc.) anche al fine di poter desumere i requisiti di onorabilità e professionalità delle controparti con le quali la Società opera;

- identificare e selezionare i fornitori e i partner commerciali secondo modalità che consentano una comparazione obiettiva e trasparente delle offerte, basata su criteri oggettivi e documentabili, verificandone l'attendibilità commerciale (ad esempio, attraverso l'acquisizione di: visure ordinarie presso la Camera di Commercio o certificato equivalente di giurisdizioni

estere; referenze da parte di altri soggetti già in rapporti con la Società o pubbliche istituzioni o associazioni professionali o studi professionali di alta reputazione; certificato antimafia o certificato carichi pendenti degli amministratori o certificati equivalenti di giurisdizioni estere, laddove possibile);
- nel caso di elargizioni di danaro ad individui, società o organizzazioni, verificare la serietà e la professionalità del destinatario;

Inoltre, AXIANS assicura che:

- nei contratti con i fornitori ed i partner commerciali sia inserita una specifica clausola con la quale gli stessi si dichiarano a conoscenza dei principi etici e comportamentali di cui al Codice Etico ed al presente Modello e si impegnano al rispetto degli stessi; il mancato rispetto dei principi e delle regole di condotta enunciate nel Modello e/o nel Codice Etico di Gruppo potranno comportare l'applicazione di una penale o, a seconda della gravità, la risoluzione del contratto.

B. Gestione dei flussi finanziari

In relazione alla gestione dei flussi finanziari (incassi e pagamenti), la Società si impegna a garantire che:

- non vengano accettati o effettuati pagamenti in denaro contante;
- sia effettuato un costante monitoraggio dei flussi finanziari aziendali, con particolare riferimento all'origine dei pagamenti e/o al soggetto beneficiario degli stessi; tali controlli devono tener conto della sede legale della controparte contrattuale (es. paradisi fiscali, paesi a rischio terrorismo), degli istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni) e di eventuali strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
- in caso di anomalie, il pagamento venga immediatamente bloccato;
- tutte le informazioni acquisite siano adeguatamente tracciate e archiviate;
- sia effettuato un report interno in caso di presunti incassi e/o pagamenti anomali.

5. Reporting all'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di verificare la corretta applicazione dei protocolli di cui alla presente Parte Speciale, i Responsabili delle Funzioni coinvolte nella gestione dei processi sensibili di cui al punto 2) dovranno trasmettere all'OdV le informazioni e le segnalazioni previste dalle procedure "*PMOG02 ODV Procedura Flussi informativi*" e "*PMOG01 Procedura Segnalazione Violazioni Whistleblowing*".

Parte Speciale 9

Reati ambientali

La presente Parte Speciale si riferisce ai reati di cui all'art. 25-undecies del Decreto, come dettagliatamente definiti nell'**Allegato A**.

1. I reati ambientali (art. 25-undecies del D. Lgs. 231/2001)

AXIANS non possiede stabilimenti produttivi e, pertanto, la stessa produce pochi rifiuti, prevalentemente rifiuti solidi urbani e rifiuti derivanti dallo svolgimento delle ordinarie attività aziendali (i.e. dispositivi informatici obsoleti o non più utilizzabili, imballaggi, rifiuti derivanti dalle attività di manutenzione e assistenza effettuate per conto dei clienti, ecc.). Per quanto riguarda i primi, la Società ha adottato un sistema di raccolta differenziata. I rifiuti speciali assimilati agli urbani (carta e cartone, plastica, indifferenziata, ecc.) vengono anch'essi smaltiti attraverso il servizio di raccolta gestito dal Comune o da ditte specializzate per gestione rifiuti da magazzino.
La Società è iscritta all'albo dei gestori ambientali e possiede un'autorizzazione per le operazioni di raccolta e trasporto di rifiuti non pericolosi (codici CER 15.01.01 - imballaggi in carta e cartone - CER 15.01.02 - imballaggi in plastica - e CER 15.01.03 - imballaggi in legno). I rifiuti pericolosi e quelli che non possiedono la classificazione CER indicata vengono invece smaltiti attraverso terzi autorizzati.
Si precisa, inoltre, che la Società non produce immissioni atmosferiche o acque reflue.
La Società garantisce la gestione della tracciabilità dei rifiuti attraverso il sistema RENTRI (Registro Elettronico Nazionale per la Tracciabilità dei Rifiuti), assicurando la registrazione dei movimenti di carico e scarico entro i termini normativi, l'emissione e gestione in formato digitale dei Formulari di Identificazione Rifiuto (FIR) e la corretta archiviazione dei dati. Il Responsabile QHSE è responsabile della continuità e conformità dell'iscrizione al RENTRI.
Axians è certificata sulla base della norma UNI ISO 14001: 2015.
Ciò premesso, in considerazione dell'analisi dei rischi effettuata e della specifica attività svolta dalla Società, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati ambientali:

- Inquinamento ambientale (art. 452-bis c.p.)
- Disastro ambientale (art. 452-quater c.p.)
- Delitti colposi contro l'ambiente (art. 452-quinquies c.p.)
- Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.)
- Circostanze aggravanti (art. 452-octies c.p.);
- Attività di gestione di rifiuti non autorizzata (art. 256 D.Lgs. 152/2006)
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 D.Lgs. 152/2006)
- Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.)

- Traffico illecito di rifiuti (art. 259 D.Lgs 152/2006)
- Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260-bis D. Lgs. 152/2006)
- Sanzioni (art. 279 D.Lgs. 152/2006).

Per una disamina approfondita dei reati sopra elencati e delle sanzioni applicabili all'ente si rimanda all'**Allegato A**.

2. Attività sensibili

In relazione ai reati ambientali di cui all'art. 25-undecies del Decreto, sono stati ritenuti maggiormente a rischio i seguenti processi:

A) gestione dei rifiuti;

B) selezione dei fornitori/imprese appaltatrici.

I principali protocolli di controllo definiti dalla procedura sono i seguenti:

1. Classificazione e identificazione dei rifiuti

La corretta attribuzione del codice CER a ciascuna tipologia di rifiuto prodotto è effettuata dal Datore di Lavoro o suo incaricato, in collaborazione con il Responsabile Logistica, secondo i criteri gerarchici previsti dalla normativa. Ove necessario, la classificazione è supportata da analisi chimiche presso laboratori accreditati. È fatto espresso divieto di abbandonare materiali o imballaggi in aree diverse da quelle deputate al corretto smaltimento.

2. Raccolta differenziata e deposito temporaneo

I rifiuti sono raccolti e stoccati in aree di deposito temporaneo appositamente individuate, in contenitori idonei — cassoni in plastica, fusti in acciaio — identificati mediante idonea cartellonistica riportante tipologia e codice CER. I rifiuti pericolosi e non pericolosi sono fisicamente separati. I limiti temporali e quantitativi previsti dalla normativa (avvio a recupero/smaltimento almeno trimestrale per i pericolosi, semestrale per i non pericolosi, con limiti volumetrici rispettivamente di 10 m^3 e 20 m^3) sono rigorosamente rispettati.

3. Verifica dei fornitori e conferimento a terzi

Il conferimento dei rifiuti è effettuato esclusivamente a soggetti in possesso delle necessarie autorizzazioni. Prima della contrattualizzazione di ciascuna impresa incaricata, il Responsabile QHSE effettua una verifica preventiva delle autorizzazioni. Le autorizzazioni di trasportatori, smaltitori e recuperatori — con controllo della data di scadenza e della coerenza tra codici CER autorizzati e rifiuti conferiti — sono archiviate e monitorate tramite il software gestionale Atlantide, che garantisce altresì l'integrazione con il sistema RENTRI e la predisposizione del MUD.

4. Adempimenti dichiarativi — MUD

Annualmente, entro il 30 aprile, il Datore di Lavoro o suo Delegato provvede alla redazione e

presentazione del Modello Unico di Dichiarazione (MUD) alla Camera di Commercio competente per territorio, con eventuale supporto di ditta terza autorizzata. Copia della dichiarazione è archiviata e custodita dal Responsabile QHSE.

5.) Gestione dei rifiuti presso clienti

I rifiuti prodotti nell'ambito di attività di manutenzione o assistenza presso siti di clienti sono considerati, ai sensi della normativa vigente, prodotti presso la sede dell'impresa. I rifiuti non pericolosi possono essere trasportati presso la sede aziendale esclusivamente se rientranti tra i codici CER autorizzati e mediante mezzi aziendali iscritti all'Albo Gestori Ambientali (categoria 2-bis). I rifiuti pericolosi eventualmente prodotti presso il cliente restano nel sito fino al ritiro da parte di un trasportatore terzo autorizzato.

6. Controllo periodico e non conformità

Il Responsabile QHSE, unitamente al Responsabile di Magazzino, effettua ispezioni trimestrali nelle aree di deposito, registrate sull'apposita modulistica (MDGS82 – Registro di Verifica Gestione Rifiuti). Le anomalie rilevate — contenitori danneggiati, errata separazione, documentazione incompleta, mezzi non conformi — sono segnalate tempestivamente, registrate, analizzate e gestite mediante azioni correttive e preventive nel rispetto del Sistema di Gestione Ambientale ISO 14001.

3. Principi generali di comportamento

Nell'espletamento delle proprie attività e funzioni, oltre a conoscere e rispettare i principi dettati dal Codice Etico, da ogni *policy* di Gruppo e procedura operativa o normativa interna adottata dalla Società, i Destinatari sono tenuti a:

a) vigilare, per quanto di competenza, sul rispetto degli adempimenti in materia ambientale, in particolare sull'osservanza delle norme operative sul raggruppamento e deposito temporaneo dei rifiuti secondo la loro classificazione e sulla consegna ai trasportatori incaricati;
b) astenersi dall'affidare incarichi/appalti a consulenti esterni e/o fornitori eludendo criteri documentabili e obiettivi incentrati su professionalità qualificata, competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta devono ispirarsi ai criteri di chiarezza e trasparenza dettati dal Codice Etico di Gruppo;
c) nell'ambito delle procedure acquisitive di prodotti, macchine e attrezzature, che a fine ciclo vita potrebbero essere classificati potenzialmente pericolosi per l'ambiente, ottenere preventivamente dal potenziale fornitore la "*scheda di sicurezza/pericolosità del prodotto*" ed il codice CER da utilizzare per il corretto smaltimento dello stesso;
d) adottare una condotta trasparente e collaborativa nei confronti delle autorità pubbliche preposte al controllo (es, ASL., Vigili del Fuoco, ARPA, Comune, Provincia, ecc.) in occasione di accertamenti/procedimenti ispettivi;
e) osservare le disposizioni di legge, la normativa interna e le istruzioni impartite dalle autorità competenti;
f) segnalare immediatamente al soggetto preposto al proprio ufficio qualsiasi situazione di

emergenza ambientale;

g) Verificare che, durante il trasporto di rifiuti con mezzi aziendali, siano rispettate tutte le prescrizioni previste dall'autorizzazione all'Albo Nazionale Gestori Ambientali.

4. Protocolli specifici di comportamento

Al fine di garantire il rispetto della normativa in materia ambientale e il corretto espletamento degli adempimenti connessi alla gestione dei rifiuti, in aggiunta a quanto previsto dal presente Modello, dalle *policy* e dal Codice Etico del Gruppo Vinci, AXIANS ha altresì implementato le seguenti procedure/istruzioni operative:

- PDSG12_Gestione rifiuti;

Si prevedono, inoltre, i seguenti protocolli di comportamento:

A. Gestione dei rifiuti

In relazione all'attività di gestione dei rifiuti, AXIANS garantisce che:

- siano individuati i soggetti responsabili della tematica ambientale e della gestione dei rifiuti (in particolare: Responsabile *QHSE*, Datore di Lavoro e Responsabile della Logistica);
- la produzione, detenzione, classificazione e conferimento rifiuti venga effettuata nel pieno rispetto della normativa ambientale, in modo da poter certificare l'attuazione dei necessari adempimenti agli organismi pubblici preposti ai controlli; in particolare, l'assegnazione del codice CER al rifiuto è effettuata a cura del Datore di Lavoro da un suo incaricato, in collaborazione con il Responsabile della Logistica;
- in conformità a quanto previsto dalla procedura "*PDGS12_Gestione rifiuti*", i rifiuti prodotti siano (i) collocati in appositi contenitori (cassoni in plastica, fusti in acciaio, ecc.) contrassegnati da idonea cartellonistica, recante l'indicazione del rifiuto da conferire ed il relativo codice CER (ii) raggruppati in apposite aree di deposito temporaneo e (iii) smaltiti dai soggetti autorizzati;
- è assolutamente vietato abbandonare o depositare rifiuti, materiali, imballaggi ecc. al di fuori dell'apposita area adibita al deposito temporaneo dei rifiuti;
- in caso di attività svolte presso clienti, il personale aziendale provvede alla presa in carico dei rifiuti derivanti dalla propria attività e garantisce la corretta gestione degli stessi nel rispetto della normativa vigente. I rifiuti classificati come non pericolosi possono essere trasportati presso la sede aziendale, a condizione che: rientrino tra i codici CER autorizzati e il trasporto avvenga mediante mezzi aziendali iscritti all'Albo Gestori Ambientali (cat. 2-bis). In caso di produzione di rifiuti pericolosi presso il cliente, non essendo l'impresa autorizzata al trasporto di tale tipologia di rifiuti, il ritiro deve essere effettuato da un trasportatore terzo autorizzato. Il rifiuto resta presso il sito del cliente fino al ritiro;
- siano previsti tempi massimi per il deposito temporaneo dei rifiuti nelle apposite aree: in particolare, in conformità a quanto previsto dalla procedura "*PDGS12_Gestione rifiuti*", i rifiuti pericolosi devono essere avviati alle operazioni di recupero o smaltimento con cadenza almeno trimestrale (o al raggiungimento del volume di 10 m3), mentre i rifiuti non pericolosi con

cadenza almeno semestrale (o quando siano raggiunti i 20 m3 di volume).

- siano previsti controlli periodici sulla corretta gestione dei rifiuti in azienda, mediante appositi sopralluoghi effettuati a cura del Responsabile QHSE (o di un soggetto da questi appositamente delegato);
- Periodicamente (controllo trimestrale) Il Responsabile QHSE o suo incaricato, insieme al Responsabile del Magazzino effettuano un'ispezione in campo per valutare che la gestione dei rifiuti sia effettuata correttamente. Il controllo deve essere registrato sull'apposita modulistica;
- sia compilato, qualora sia necessario, in modo corretto e veritiero, il registro di carico e scarico ed il formulario di identificazione per il trasporto dei rifiuti ("FIR"), astenendosi dal porre in essere operazioni in falso ideologico o materiale (ad esempio in relazione alle informazioni sulle caratteristiche qualitative o quantitative dei rifiuti), nonché qualsiasi altra documentazione richiesta per legge;
- tutta la documentazione ambientale richiesta per legge ed i relativi formulari sia custodita accuratamente in apposito archivio presso la sede della Società.

B. Selezione dei fornitori/imprese appaltatrici

Il ricorso ad *outsourcer* terzi nelle attività di recupero, trasporto e smaltimento richiede:

- la puntuale verifica, ad opera del Datore di Lavoro e della funzione QHSE, circa la sussistenza delle autorizzazioni e/o delle iscrizioni all'albo in capo agli smaltitori/trasportatori;
- l'inserimento, nei contratti con tali soggetti, di clausole volte a disciplinare le conseguenze della violazione da parte degli stessi della normativa in materia ambientale, nonché delle disposizioni di cui al Decreto e dei principi contenuti nel presente Modello.

Inoltre:

- è assolutamente vietato consegnare i rifiuti speciali a trasportatori/smaltitori che non siano censiti nell'elenco delle Società autorizzate alla gestione dei rifiuti presente sulla intranet aziendale.

5. Reporting all'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di verificare la corretta applicazione dei protocolli di cui alla presente Parte Speciale, i Responsabili delle Funzioni coinvolte nella gestione dei processi sensibili di cui al punto 2) dovranno trasmettere all'OdV le informazioni e le segnalazioni previste dalle procedure "*PMOG02 ODV Procedura Flussi informativi*" e "*PMOG01 Procedura Segnalazione Violazioni Whistleblowing*".

Parte Speciale 10

Reati tributari

La presente Parte Speciale si riferisce ai reati di cui all'art. 25-quinquesdecies del Decreto, come dettagliatamente definiti nell'**Allegato A**.
Tale categoria di Reati Presupposto è stata introdotta dal D.L. n. 124/2019 (convertito in Legge n. 157/2019) e successivamente ampliata ad opera del D.Lgs. n. 75/2020, che - in attuazione della Direttiva (UE) 2017/1371 (c.d. Direttiva PIF) concernente la lotta contro le frodi che ledono gli interessi finanziari dell'Unione - ha disposto l'inclusione nel Decreto di ulteriori fattispecie di reato previste dal D.Lgs. n. 74/2000, qualora le stesse siano commesse nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto (IVA) per un importo complessivo non inferiore a Euro 10 milioni, ossia i reati di dichiarazione infedele (art. 4, D.Lgs. n. 74/2000), omessa dichiarazione (art. 5, D.Lgs. n. 74/2000) e indebita compensazione (art. 10-quater, D.Lgs. n. 74/2000).

1. I reati tributari (art. 25-quinquesdecies del D. Lgs. 231/2001)

In considerazione della mappatura dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati:

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, D.Lgs. 74/2000);
- Dichiarazione fraudolenta mediante altri artifici (art. 3, D.Lgs. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, D.Lgs. 74/2000);
- Occultamento o distruzione di documenti contabili (art. 10, D.Lgs. 74/2000);
- Sottrazione fraudolenta al pagamento di imposte (art. 11, D.Lgs. 74/2000);
- Dichiarazione infedele (art. 4, D.Lgs. 74/2000);
- Omessa dichiarazione (art. 5, D.Lgs. 74/2000);
- Indebita compensazione (art. 10-*quater*, D.Lgs. 74/2000).

Per una disamina approfondita dei reati sopra elencati e delle sanzioni applicabili all'ente si rimanda all'**Allegato A**.

2. Attività sensibili

In relazione alle fattispecie richiamate nella presente Sezione di Parte Speciale, le attività che la Società ha individuato come maggiormente sensibili sono:

A) gestione degli adempimenti contabili e fiscali;
B) rapporti con i clienti e ciclo attivo;
C) operazioni straordinarie (es. cessione dell'azienda o di un ramo di essa, acquisizioni, scissioni, ecc.) e dismissione di cespiti;
D) gestione del personale (adempimenti retributivi, contributivi e previdenziali, gestione delle carte di credito aziendali);

E) gestione delle note spese e delle spese di rappresentanza;
F) approvvigionamento di beni e servizi e ciclo passivo;
G) gestione magazzino;
H) gestione delle sponsorizzazioni e concessione di donazioni, omaggi e liberalità;
I) gestione dei finanziamenti (pubblici e non);
J) gestione dei flussi finanziari, della cassa aziendale e rapporti infragruppo.

3. Principi generali di comportamento

Nell'espletamento delle proprie attività e funzioni, oltre a conoscere e rispettare i principi dettati dal Codice Etico, da ogni *policy* di Gruppo e procedura operativa o normativa interna adottata dalla Società, i Destinatari sono tenuti a:

a) rispettare le norme in materia fiscale e tributaria applicabili alla Società; in particolare, le registrazioni contabili devono essere effettuate nel rispetto dei principi contabili vigenti ed essere complete e veritiere;
b) rispettare le procedure e le prassi interne adottate dalla società in materia di ciclo attivo e passivo e flussi finanziari al fine di consentire la ricostruibilità ex post di tutte le operazioni;
c) garantire il monitoraggio e l'aggiornamento costante dell'anagrafica dei fornitori di beni e servizi e l'anagrafica dei clienti;
d) verificare l'effettività delle prestazioni rese o ricevute; a tal fine, tutte le fatture ricevute o emesse devono essere approvate e autorizzate secondo il sistema di deleghe e procure in essere;
e) segnalare eventuali criticità o anomalie relative ai processi finanziari (es. incongruenza della fattura rispetto all'ordine, non corrispondenza del soggetto che ha emesso la fattura con il fornitore registrato in anagrafica, anomalia dei prezzi dei beni acquistati, ecc.);
f) tenere la contabilità in modo da consentire, in qualunque momento, la ricostruzione dei redditi e del volume d'affari;
g) verificare la correttezza e completezza dei dati riportati nelle dichiarazioni fiscali prima di sottoporle alla firma del legale rappresentante;
h) in caso di alienazione di beni e/o operazioni straordinarie, le stesse devono essere sottoposte ad un processo di approvazione interno; in particolare occorre valutare (i) le ragioni di opportunità commerciale e/o economica nell'effettuare l'operazione, (ii) la congruità del corrispettivo dell'operazione, (iii) l'identità delle controparti coinvolte ed eventuali rapporti di parentela con soci/amministratori, (iv) il reale interesse delle controparti all'operazione, (v) la frequenza nel tempo delle operazioni di alienazione e cessione, nonché (vi) la situazione di eventuali debiti verso l'erario;
i) prevedere incontri periodici tra l'OdV e il Collegio Sindacale/Revisori al fine di promuovere uno scambio reciproco di informazioni relative alle aree sensibili sopra indicate.

Inoltre, è fatto divieto ai Destinatari di:

j) intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo, persone legate all'ambiente del riciclaggio

k) utilizzare strumenti che non siano proceduralizzati e tracciabili per il compimento di operazioni di trasferimento di denaro;
l) emettere e/o annotare in contabilità fatture o altri documenti equipollenti per operazioni (soggettivamente o oggettivamente) inesistenti;
m) avvalersi di documentazione falsa o di altri mezzi fraudolenti idonei ad ostacolare le attività di accertamento e/o ad indurre in errore l'amministrazione finanziaria;
n) occultare, anche solo temporaneamente, o distruggere i documenti o le scritture contabili al fine di impedire la ricostruzione dei redditi o del volume d'affari;
o) effettuare atti di alienazione simulata o altri atti fraudolenti al fine di sottrarsi al pagamento delle imposte;
p) indicare nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo oppure elementi passivi fittizi.

4. Protocolli specifici di comportamento

Ad integrazione delle norme di comportamento di cui sopra ed al fine di fornire un dettaglio operativo rispetto ai principi già declinati nei Codici e nelle *policy* di Gruppo, la Società ha formalizzato le specifiche procedure e istruzioni operative aventi ad oggetto alcuni dei processi a rischio identificati:

- PRO01_Bidding Procedure;
- IOP03_Gestione approvazione Pricesheet;
- PRO02_Gestione commesse;
- PUPG01_Gestione della progettazione e sviluppo prodotti e servizi;
- PUAC02_Gestione del magazzino;
- PMOG03_Gestione Omaggi & Inviti;
- PURU01_Gestione della ricerca e della selezione del personale;
- PURU03_Gestione e sviluppo delle risorse umane;
- PDSG11_Gestione Trasferte Estero;
- PURU10_Travel policy;
- PRO11_ Pre sales procedure;
- PRO15_Valutazione fornitori;
- PRO13_Gestione degli Acquisti;
- PMOG05_Procedura Gestione Flussi Finanziari ed Economici.

In aggiunta ai principi di cui sopra, si prevedono i seguenti protocolli specifici di comportamento:

A. Gestione degli adempimenti contabili e fiscali

In relazione alla predisposizione del bilancio (anche consolidato), alla tenuta delle altre scritture contabili e alla predisposizione delle dichiarazioni fiscali, si prevede che:

- deve essere effettuato il monitoraggio della regolare tenuta delle scritture contabili aziendali ad opera delle funzioni aziendali (*Finance & Administration*) e degli organi di controllo (Sindaci/Revisori) al fine di verificare la corretta e fedele rappresentazione della situazione economico-finanziaria della società e del bilancio civilistico e consolidato;
- deve essere tenuto uno scadenziario degli adempimenti fiscali e contributivi, anche con il supporto del consulente esterno incaricato;
- deve essere effettuato un monitoraggio della normativa fisale applicabile alla società anche con il supporto del commercialista esterno;
- le bozze del bilancio civilistico, delle dichiarazioni e dei modelli per il pagamento delle imposte sono predisposte con il supporto del consulente esterno, sottoposte alla verifica degli organi di controllo (Sindaci/Revisori) e, infine, alla firma del legale rappresentante della società;
- la dichiarazione dei redditi, dopo verifica e benestare dei Revisori e firma del legale rappresentante, deve essere trasmessa al commercialista con delega per la presentazione all'agenzia delle entrate.
- le scritture contabili devono essere correttamente registrate a cura dell'Amministrazione e condivise con il commercialista.

B. Rapporti con i clienti e ciclo attivo

In conformità alle procedure interne e alla prassi operativa:

- è mantenuta un'anagrafica dei clienti a sistema che viene gestita e costantemente aggiornata dal *Customer Care* (CC) ed è collegata al CRM (*Salesforce*);
- i rapporti con i clienti siano formalizzati per iscritto; per clienti di maggiori dimensioni, vengono stipulati appositi contratti quadro mentre, in caso di PMI, è comunque richiesta la sottoscrizione delle Condizioni Generali di Contratto contenenti clausole di accettazione del Codice Etico e del Codice di Condotta Anticorruzione di VINCI e del Modello 231 di AXIANS;
- i contratti con i clienti sono approvati e sottoscritti dai soggetti aziendali dotati di idonei poteri di rappresentanza;
- l'intero processo di gestione della commessa è tracciato tramite gestionale, sul quale sono caricati tutti i dati amministrativi e finanziari dell'ordine e del cliente, nonché le fasi di progetto, le note operative e i rapporti e controlli del *team Delivery*. Il gestionale traccia, altresì, il flusso approvativo proveniente dalle funzioni *Sales* e CC;
- in particolari casi in cui vi sia rischio di corruzione alto (ad es. per valori di progetto particolarmente rilevanti ovvero per area territoriale ad alto rischio corruttivo o per coinvolgimento di persone politicamente esposte o per altre ragioni), vengono effettuate verifiche sulla onorabilità morale (cfr. *Procedura Risk Assessment Terze Parti*) e solidità economico-finanziaria dei clienti, anche attraverso *provider* esterni (*Cerved*); in caso di nuovi clienti viene chiesto il versamento di un anticipo, pari al 30% del valore della commessa; eventuali deroghe a tale procedura richiedono la preventiva autorizzazione dell'AD o di altro soggetto munito dei necessari poteri;
- l'offerta nei confronti dei clienti è formalizzata per iscritto, anche sulla base della valutazione economico finanziaria della commessa; in caso di appalti da parte di Fincantieri, la Società riceve da Fincantieri una richiesta di quotazione (c.d. "*reference quotation*") e assegna al progetto un

budget sulla base di una stima interna dei costi e degli utili.

- è prevista una verifica sulla corretta esecuzione delle prestazioni rispetto ai termini ed alle condizioni pattuite, nonché la corrispondenza della fattura all'ordine; in particolare: (i) se l'ordine ha per oggetto la consegna di beni, il *team Delivery* carica a sistema la DDT a comprova della spedizione della merce al cliente e cambia stato alla commessa e il CC emette contestualmente la fattura al cliente (ii) per offerte a progetto, è nominato un coordinatore del progetto che definisce i tempi di realizzazione del progetto e individua il *Project Manager* incaricato. Il *Project Manager* (PM) dà al CC l'input per la fatturazione al raggiungimento delle *milestones*; al termine del progetto, il tecnico incaricato inserisce a sistema un rapporto (*timesheet*) con le ore e le attività eseguite; (iii) per contratti di assistenza, il CC inserisce a sistema il piano dei pagamenti concordati ed ogni fine mese estrapola le fatture da emettere;
- Il CC ha visibilità anche degli ordini caricati a sistema dall'Ufficio Acquisti connessi con lo specifico ordine (es. se è necessario acquistare dei materiai o servizi per realizzare la commessa);
- le fatture attive sono emesse dal *Customer Care* (CC) secondo quanto contrattualmente stabilito con il cliente; Il processo di fatturazione è gestito tramite gestionale, sul quale il CC carica l'ordine e tutta la documentazione relativa (es. fattura, *pricesheet* ecc.). La documentazione proveniente dall'esterno (es. mail contenente l'ordine del cliente) è invece caricata su un *link* direttamente associato all'ordine cui fa riferimento. Per la registrazione a sistema degli ordini di importo superiore a 500 euro, è sempre necessario che vi sia un ordine scritto (mail) del cliente;
- eventuali richieste di rettifica fatture e note di credito siano approvate secondo il sistema di deleghe in essere, previa verifica della fondatezza della richiesta;
- eventuali solleciti di pagamento sono gestiti dalla funzione *Finance*, con l'eventuale supporto di un legale esterno, laddove necessario.

C. Operazioni straordinarie (es. cessione dell'azienda o di un ramo di essa, acquisizioni, scissioni, ecc.) e dismissione di cespiti

In relazione a tale area sensibile, si prevede che:

- sia necessario espletare attività di *due diligence* per la verifica dei presupposti di carattere strategico, economico e finanziario nonché degli eventuali rischi connessi all'operazione, anche ai fini di una valutazione di fattibilità della stessa, ad opera delle competenti funzioni aziendali, nonché di consulenti esterni con funzioni di supporto (società di revisione o società terze);

- si debba effettuare una verifica preventiva di eventuali conflitti di interesse in capo alla controparte;

- l'operazione deve essere autorizzata dai soggetti dotati dei necessari poteri di firma;

- sia verificata ex post la corrispondenza tra la proposta dell'operazione autorizzata, i contenuti del contratto cui si è pervenuti a seguito delle attività negoziali e quanto effettivamente realizzato;

- sia previsto il coinvolgimento delle competenti funzioni fiscali aziendali e dei consulenti esterni incaricati, sia in fase di definizione della proposta di realizzazione dell'operazione, che nelle successive fasi di esecuzione, al fine di garantire che le operazioni siano svolte in conformità alla normativa fiscale di riferimento.

D. Gestione del personale (adempimenti retributivi, contributivi e previdenziali, gestione delle carte di credito aziendali)

La Società ha esternalizzato le attività di *payroll* (elaborazione dei cedolini e predisposizione delle dichiarazioni contributive) ad uno studio paghe esterno, al quale è stato conferito apposito incarico scritto. Inoltre, la Società si avvale del supporto di un consulente del lavoro esterno per l'analisi delle questioni giuslavoristiche e la gestione di eventuali contenziosi del lavoro (ad esempio, con organismi sindacali, D.d.l., INPS, INAIL ecc.). Ciò premesso, AXIANS assicura che:

- è mantenuta aggiornata l'anagrafica dei dipendenti della Società;
- è stato implementato un sistema di consuntivazione interno delle presenze gestite tramite portale timesheet, nel quale i collaboratori riportano le ore di lavoro distinte per commessa e attività, eventuali richieste di ferie e/o permessi e la consuntivazione delle note spese;
- è previsto un duplice controllo sulle richieste di cui sopra: le stesse sono approvate dal Responsabile di funzione e, successivamente, la funzione HR verifica che l'approvazione sia stata rilasciata;
- le buste paga e gli F24 sono predisposti dal consulente paghe sulla base di un report delle presenze, che viene elaborato mensilmente dalla funzione HR estraendo i dati dal sistema; i cedolini sono condivisi in anteprima con la funzione HR, che ne verifica la correttezza; il prospetto dei contributi da versare è invece trasmesso al CFO, che provvede a verificarne la correttezza prima dell'invio all'ente previdenziale;
- il pagamento delle retribuzioni avviene tramite bonifico bancario, previa verifica della correttezza dei dati riportati a cedolino e previa autorizzazione del CFO;
- l'Amministrazione verifica la corrispondenza tra il flusso di pagamento e l'importo indicato nelle buste paga e provvede alle registrazioni contabili;
- il sistema premiante e incentivante è basato su obiettivi prestabiliti sia economico-finanziario di risultato della BU, sia personali quantitativi (es. numero di ordini chiusi dal dipendente) sia qualitativi. che vengono definiti di concerto dai *BU Manager* e dai Responsabili di funzione alle loro dipendenze e successivamente approvati dall'AD;
- è previsto un duplice controllo sul raggiungimento degli obiettivi ai fini dell'assegnazione di premi/incentivi/bonus: una prima verifica da parte del *BU Manager* di riferimento ed una ulteriore verifica ad opera dell'AD, con l'eventuale supporto di *Finance*. Una volta approvato il premio, HR predispone una lettera da sottoporre al dipendente per sottoscrizione e nella quale viene indicato l'obiettivo raggiunto.

E. Gestione delle note spese e delle spese di rappresentanza

In coerenza con quanto previsto dalla "*PURU10_Travel Policy*", dalla " *PURU03 Procedura Gestione e sviluppo delle Risorse Umane*" e dalla procedura "*PMOG03_Gestione Omaggi & Inviti:*

- la richiesta di rimborso spese deve essere presentata dal dipendente compilando l'apposito modulo nota spese e allegando ad esso i giustificativi di spesa;
- la nota spese deve quindi essere approvata dal Responsabile di funzione del richiedente e successivamente verificata dall'Amministrazione;
- l'HR riceve un *report* con evidenza delle note spese presentate da ogni dipendente e delle eventuali spese di rappresentanza e lo trasmette, dopo le opportune verifiche, al consulente paghe per il rimborso a cedolino;
- è possibile erogare il rimborso spese ai dipendenti in denaro contante solo in via d'eccezione e, in ogni caso, dietro presentazione di idonei giustificativi di spesa;
- l'Amministrazione provvede a contabilizzare correttamente nel sistema informativo aziendale (*Navision*) i dati relativi alle note spese;
- tutta la documentazione relativa alle note spese deve essere opportunamente archiviata.

F. Approvvigionamento di beni e servizi e ciclo passivo

In relazione all'approvvigionamento di beni e servizi e alla gestione del ciclo passivo, in conformità alle procedure "*PRO14_Gestione della logistica e del magazzino*" e "*PRO13_Gestione degli acquisti*" e alla prassi internamente seguita, si prevede che:

- i rapporti con i fornitori e altri soggetti terzi devono sempre essere formalizzati per iscritto (tramite contratto o ordine) ed essere approvati e sottoscritti secondo il sistema di deleghe/procure adottato dalla Società;
- prima del pagamento dell'ordine deve essere effettuato il confronto tra ordine, fattura e conferma della ricezione del bene/servizio, sia in termini qualitativi che quantitativi; in particolare, il magazzino verifica la corrispondenza tra il DDT e la merce consegnata e che la merce ricevuta corrisponda all'ordine in termini di quantità e qualità, carica l'entrata merce a sistema e trasmette il DDT all'Ufficio Acquisti. Quest'ultimo, a sua volta, verifica la corrispondenza ordine/fattura ed approva il pagamento;
- in caso di acquisti riferiti ad uno specifico progetto, l'Ufficio Acquisti convalida il pagamento della fattura solo dopo avere acquisito il benestare del PM rispetto all'esecuzione dei lavori e/o alla corrispondenza del DDT di consegna;
- qualora vengano riscontrate anomalie, l'Ufficio Acquisti blocca il pagamento in attesa che la non conformità venga risolta;
- tutta la documentazione relativa all'ordine (carico, fattura fornitore, ecc.) è caricata sull'ERP aziendale (*Navision*); il DDT di entrata è archiviato in modalità cartacea e allegato alla copia

della fattura di acquisto registrata in contabilità;

- i servizi di consulenza e gli appalti di servizi (es. pulizie) sono regolati da un contratto quadro e la conferma dell'effettività della prestazione è data, nel primo caso, dal richiedente, nel secondo caso da una funzione ad hoc responsabile degli immobili;
- la conferma dell'attività svolta da agenti/procacciatori è acquisita a monte, con la trasmissione dell'ordine da parte del cliente. Le provvigioni degli agenti sono liquidate in base al contratto e la loro entità diminuisce in funzione degli sconti applicati al cliente;
- prima di ogni pagamento, deve essere raccolta la doppia firma approvativa dei soggetti legittimati come da file "*Poteri*" (es. AD e/o procuratore speciale);
- tutti i pagamenti ai fornitori e terzi in genere (consulenti, agenti ecc.) sono effettuati tramite carta di credito o bonifico bancario e possono, pertanto, essere ricostruiti ex post.

G. Gestione magazzino

In conformità alla procedura "*PRO14_Gestione della logistica e del magazzino*":

- è garantita la tracciabilità dei flussi logistici di magazzino in entrata e in uscita;
- viene effettuato un controllo ed un aggiornamento periodico dell'inventario per verificare la corrispondenza della quantità contabile di magazzino con la quantità fisica effettiva in giacenza;
- è garantito il monitoraggio delle giacenze in magazzino;
- eventuali rettifiche inventariali devono essere approvate da soggetti dotati dei necessari poteri autorizzativi.

G. Gestione dei finanziamenti (pubblici e non)

Si osservano, in quanto compatibili, i protocolli di cui alla sezione A) Rapporti con la Pubblica Amministrazione, al punto A.2.

H. Gestione delle sponsorizzazioni e concessione di donazioni, omaggi e liberalità

Conformemente a quanto stabilito dalle *policy* di Gruppo e dalla procedura Procedura "*PMOG03_Gestione Omaggi & Inviti*":

- tutte le liberalità devono essere gestite in modo trasparente; le stesse devono avere scopo caritatevole o essere volte alla promozione dell'immagine della Società e/o all'esposizione del marchio; non sono ammesse donazioni e liberalità a favore di enti o associazioni con finalità di lucro;
- sponsorizzazioni e liberalità possono essere deliberate esclusivamente dall'organo

amministrativo (CdA o AD munito dei necessari poteri), anche su richiesta del *BU Manager*; omaggi, le ospitalità e pranzi/cene professionali sono decisi dal *BU Manager* in coerenza con il budget assegnato alla BU e secondo i criteri indicati nelle "*Guidelines Omaggi e Inviti Vinci Energies Italia*" e riportati nella procedura interna "*PMOG03_Gestione Omaggi & Inviti;*

- le sponsorizzazioni possono essere volte a sostenere iniziative di valore umanitario e sociale, riguardare eventi ed iniziative a carattere sociale, culturale, sportivo ed artistico, studi, ricerche, convegni e seminari di rilevanza sociale e di interesse per la Società. In ogni caso, i rapporti di sponsorizzazione devono essere contrattualizzati;
- sono vietate liberalità/sponsorizzazioni e omaggi in denaro contante, indipendentemente dall'importo;
- le spese relative a pranzi/cene di lavoro devono essere rendicontate mensilmente al *BU Manager* di riferimento ed essere documentate; il *BU Manager* verifica che la spesa sia coerente con la documentazione a corredo e ne autorizza il rimborso entro i limiti di budget annuale assegnatogli dal CdA;
- l'elargizione materiale dell'erogazione liberale/donazione può essere effettuata esclusivamente dalla funzione *Finance & Administration*, previa approvazione dell'Amministratore Delegato o del Presidente del CdA;
- deve essere garantita la tracciabilità degli importi erogati, dei beneficiari e degli scopi della donazione; a tal fine, viene predisposto internamente un report degli omaggi elargiti e ogni donazione è registrata nei libri contabili della Società;
- la documentazione relativa ad omaggi, sponsorizzazioni, ospitalità è conservata negli archivi della Società per un periodo di almeno 10 anni.

I. Gestione dei flussi finanziari, della cassa aziendale e rapporti infragruppo.

Con riferimento a tale area sensibile, si prevede che:

- sono vietati pagamenti in contanti, salvo quanto previsto dalle *policy* interne e di Gruppo per la gestione della piccola cassa;
- i pagamenti devono essere autorizzati dai soggetti dotati di idonei poteri, secondo il sistema di deleghe in vigore; in particolare, conformemente alle *policy* di Gruppo, è necessaria l'approvazione congiunta del Presidente del CdA e dell'Amministratore Delegato di AXIANS;
- prima di predisporre i pagamenti, deve essere verificata i) la coerenza delle fatture rispetto agli ordini ii) l'effettiva esecuzione delle prestazioni/ricezione di beni, secondo le modalità previste dalle procedure adottate dalla società e dalla prassi operativa vigente;
- le fatture verso i clienti possono essere emesse solo dopo la verifica dell'effettiva esecuzione della prestazione in conformità agli accordi presi con il cliente;
- devono essere effettuate riconciliazioni periodiche dei conti correnti al fine di garantire il monitoraggio dei flussi finanziari e verificare la corrispondenza tra pagamenti e fatture ricevute, nonché tra incassi e fatture emesse. È inoltre previsto un controllo di secondo livello ad opera

dei Sindaci/Revisori;
- i pagamenti possono essere effettuati esclusivamente tramite bonifico bancario o altri strumenti di pagamento documentabili;
- i flussi finanziari aziendali sono costantemente monitorati, con particolare riferimento all'origine dei pagamenti ed al soggetto beneficiario degli stessi, anche al fine di verificare che si tratti dei soggetti effettivamente coinvolti nelle operazioni;
- tutte le informazioni acquisite e le operazioni finanziarie effettuate devono essere adeguatamente tracciate tramite i sistemi gestionali in uso e ricostruibili ex post;
- in caso di presunti incassi e/o pagamenti anomali, i Destinatari devono darne tempestiva informativa all'OdV.

Con particolare riferimento alle fatturazioni *intercompany*, AXIANS è soggetta a una serie di *fees* che rappresentano il corrispettivo di servizi resi in suo favore dalla capogruppo francese (es. prestazioni IT, consulenza informatica). AXIANS, inoltre, riconosce alla *holding* le *royalties* per l'utilizzo del *brand* di gruppo. Ciò premesso, nella gestione delle operazioni infragruppo, AXIANS garantisce che:

- i rapporti infragruppo sono formalizzati attraverso contratti di *service* infragruppo;
- le transazioni infragruppo devono essere coerenti con il valore di mercato e conformi alla normativa sul *Transfer Price* e ai documenti di supporto (*Master File* e Documentazione nazionale);
- i flussi finanziari infragruppo sono oggetto di verifiche periodiche anche al fine di verificare eventuali operazioni di compensazione crediti/debiti.

5. Reporting all'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di verificare la corretta applicazione dei protocolli di cui alla presente Parte Speciale, i Responsabili delle Funzioni coinvolte nella gestione dei processi sensibili di cui al punto 2) dovranno trasmettere all'OdV le informazioni e le segnalazioni previste dalle procedure "*PMOG02 ODV Procedura Flussi informativi*" e "*PMOG01 Procedura Segnalazione Violazioni Whistleblowing*".

Parte Speciale 11

Contrabbando e violazioni delle misure restrittive dell'Unione Europea

La presente Parte Speciale si riferisce ai reati di cui all'art. 25 sexiesdecies del Decreto e all'art. 25 octies.2, come dettagliatamente definiti nell'Allegato A.

1. Le fattispecie in materia di contrabbando (art. 25-sexiesdecies del D. Lgs. 231/2001)

Il D.lgs. 14 luglio 2020, n. 75 di recepimento della Direttiva PIF aveva inserito i reati di contrabbando doganale di cui al D.P.R. n. 43 del 23 gennaio 1973. (Testo Unico delle Leggi Doganali – "T.U.L.D.") nel catalogo dei reati che possono dare origine alla responsabilità amministrativa degli enti ai sensi del Decreto.
Tuttavia, in data 3 ottobre 2024 è stato pubblicato il Decreto Legislativo 26 settembre 2024, n. 141, recante "*Disposizioni nazionali complementari al codice doganale dell'Unione e revisione del sistema sanzionatorio in materia di accise e altre imposte indirette sulla produzione e sui consumi*" (c.d. "nuovo T.U.L.D.") che ha approvato le Disposizioni nazionali complementari al codice doganale dell'Unione, riorganizzato la disciplina in materia doganale, abrogando, tra gli altri, il T.U.L.D. (D.P.R. n. 43 del 23 gennaio 1973) e modificato quindi il testo dell'art. 25-sexiesdecies del D. Lgs. n. 231/2001 dedicato ai reati di Contrabbando.

In generale, il delitto di contrabbando consiste nell'introduzione nel territorio dello Stato, in violazione delle disposizioni in materia doganale, di merci sottoposte ai diritti di confine. Si tratta, dunque, delle fattispecie di dolosa sottrazione delle merci al pagamento dei diritti di confine.
In particolare, ai sensi dell'art. 27 del c.d. "nuovo T.U.L.D." D. Lgs. 26 settembre 2024 n. 141, si considerano "diritti doganali" tutti quei diritti che l'Agenzia delle Dogane è tenuta a riscuotere in forza di vincoli derivanti dall'ordinamento dell'Unione europea o da disposizioni di legge.
Fra i diritti doganali costituiscono "diritti di confine":

- i dazi di importazione e quelli di esportazione previsti dalla normativa unionale;
- i prelievi e le altre imposizioni all'importazione o all'esportazione previsti dai regolamenti comunitari e dalle relative norme di applicazione;
- con riferimento alle merci di importazione:
  - i diritti di monopolio;
  - le accise;
  - le sovrimposte di confine;
  - ogni altra imposta o sovrimposta di consumo a favore dello Stato;
- con riferimento all'imposta sul valore aggiunto, essa non costituisce diritto di confine nei casi di:

- immissione in libera pratica di merci senza assolvimento dell'imposta sul valore aggiunto per successiva immissione in consumo in altro Stato membro dell'Unione europea;
- immissione in libera pratica di merci senza assolvimento dell'imposta sul valore aggiunto e vincolo a un regime di deposito diverso dal deposito doganale.
- In merito alle merci soggette ai diritti di confine, il presupposto dell'obbligazione tributaria doganale è costituito, relativamente alle merci estere, dalla loro destinazione al consumo entro il territorio doganale e, relativamente alle merci nazionali e nazionalizzate, dalla loro destinazione al consumo fuori del territorio stesso.

Per quanto attiene il Decreto n. 231/2001, l'art. 25 sexiesdecies estende la responsabilità amministrativa degli enti alle fattispecie di contrabbando, previste dalle disposizioni nazionali complementari al codice doganale dell'Unione, di cui al "nuovo T.U.L.D.", e dal testo unico delle disposizioni legislative concernenti le imposte sulla produzione e sui consumi e relative sanzioni penali e amministrative, di cui al D. Lgs. 26 ottobre 1995, n. 504.

In particolare, in considerazione della mappatura dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati:

- Contrabbando per omessa dichiarazione (art. 78 D. Lgs. 141/2024);
- Contrabbando per dichiarazione infedele (art. 79 D. Lgs. 141/2024);
- Contrabbando nel movimento delle merci marittimo, aereo e nei laghi di confine (art. 80 D. Lgs. 141/2024);
- Contrabbando per indebito uso di merci importate con riduzione totale o parziale dei diritti (art. 81 D. Lgs. 141/2024);
- Contrabbando nell'esportazione di merci ammesse a restituzione di diritti (art. 82 D. Lgs. 141/2024);
- Contrabbando nell'esportazione temporanea e nei regimi di uso particolare e di perfezionamento (art. 83 D. Lgs. 141/2024);
- Contrabbando di tabacchi lavorati (art. 84 D. Lgs. 141/2024);
- Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati (art. 85 D. Lgs. 141/2024);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati (art. 86 D. Lgs. 141/2024);
- Circostanze aggravanti del contrabbando (art. 88 D. Lgs. 141/2024).

Ai sensi dell'art. 87, il tentativo di contrabbando viene equiparato al delitto consumato. Ne deriva che sarà ugualmente punita qualsiasi attività di tentata sottrazione della merce al versamento dell'obbligazione tributaria doganale.

Nello specifico contesto aziendale della Società, i reati in materia di contrabbando appaiono potenzialmente rilevanti in quanto AXIANS importa ed esporta da/verso Paesi extra UE. Le esportazioni sono più frequenti e coinvolgono tutte le BU. In entrambi i casi, la Società non ha rapporti diretti con le Dogane e si avvale di spedizionieri e dei loro operatori doganali (interni od esterni) per la gestione delle attività di sdoganamento e gli adempimenti connessi. A tal fine, la Società ha quindi conferito

agli spedizionieri mandato di rappresentanza diretta dinanzi alle Autorità Doganali. Diversamente, i rapporti con le Camere di Commercio per l'ottenimento della documentazione necessaria alle esportazioni vengono gestiti internamente. In caso di necessità, AXIANS chiede il supporto di consulenti esterni (ad esempio, per ottenere informazioni sulla normativa applicabile alle operazioni di import/export).
Con particolare riferimento alle esportazioni, la Società ha individuato al proprio interno una risorsa responsabile di garantire il corretto svolgimento di tale attività. In caso di vendita/commercializzazione di prodotti AXIANS extra UE, la Società, talvolta, consegna la merce direttamente al cliente extra UE (esportazioni "dirette"), talaltra esporta verso un cliente comunitario che, a sua volta, vende ad un cliente estero (esportazioni "indirette"). Le esportazioni dirette e indirette vengono gestite internamente se il compratore effettua il pagamento della merce tramite bonifico bancario; per le esportazioni dirette con pagamento tramite lettera di credito, la Società si avvale invece di un consulente esterno specializzato in materia.
Le attività di importazione, invece, sono gestite da una risorsa all'interno della *BU 20 Cruise*, sempre con il supporto di spedizionieri terzi.

2. Le fattispecie in materia di violazioni delle misure restrittive dell'unione europea (art. 25-octies.2 del d. lgs. 231/2001)

Il D. Lgs. 30 dicembre 2025, n. 211 di recepimento della Direttiva 2024/1226 ha introdotto nuove fattispecie penalmente rilevanti in caso di violazione di misure restrittive dell'Unione Europea. In particolar modo la novella legislativa ha ampliato il catalogo dei reati presupposto di cui al D. Lgs. 231/2001 mediante l'introduzione del nuovo art. 25-octies.2 rubricato "Reati in materia di violazione di misure restrittive dell'Unione europea".

L'intervento legislativo è infatti volto all'armonizzazione della risposta sanzionatoria degli Stati Membri alle condotte di violazione di misure restrittive dell'Unione Europea.

In particolar modo, per quanto concerne la perimetrazione delle misure restrittive, si rinvia integralmente alla disciplina dell'Unione Europea; la Società provvede al costante monitoraggio dei provvedimenti sanzionatori progressivamente adottati dalle autorità competenti tramite il sito www.sanctionsmap.eu.

In ragione di quanto sopra esposto, i reati previsti dall'art. 25-octies.2 in astratto rilevanti per la Società sono i seguenti:

a) Violazione delle misure restrittive dell'Unione Europea (art. 275-bis c.p., primo, secondo, e quinto comma);

b) Violazione di obblighi informativi imposti da una misura restrittiva dell'Unione Europea (275-ter c.p., primo e secondo comma);

c) Violazione delle condizioni dell'autorizzazione allo svolgimento di attività (art. 275-quater c.p. primo comma).

Per una disamina approfondita dei reati sopra elencati e delle sanzioni applicabili all'ente si rimanda all'**Allegato A**.

3. Attività sensibili

In relazione alle fattispecie richiamate nella presente Sezione di Parte Speciale, si ritengono maggiormente a rischio i seguenti processi:

A) gestione delle importazioni;

B) gestione delle esportazioni;

C) gestione degli adempimenti doganali;

D) gestione del magazzino.

4. Principi generali di comportamento

I dipendenti e collaboratori di AXIANS che, nell'ambito delle proprie funzioni e attività, sovraintendono o controllano le attività commerciali e/o di prestazione di servizi, le attività relative agli obblighi informativi e quelle relative al rispetto di autorizzazioni e qualsiasi altra attività che possa comportare il rispetto di misure restrittive dell'Unione Europea (ivi compresi gli operatori doganali che, attraverso la propria struttura organizzativa, dovranno garantirne il recepimento e l'osservanza nei rapporti con la Società), siano coinvolti nell'espletamento delle operazioni attinenti alla gestione dello scambio internazionale di merci, oltre a conoscere e rispettare i principi contenuti nel Codice Etico, nelle *policy* di Gruppo e in ogni altra procedura operativa o norma interna adottata dalla Società, sono tenuti a:

a) garantire l'osservanza di tutte le leggi e i regolamenti vigenti che disciplinano l'attività aziendale di commercio con l'estero;

b) gestire in modo trasparente e corretto tutte le attività finalizzate alla vendita, alla commercializzazione e allo scambio internazionale di prodotti, nonché allo scarico e deposito merci;
c) fornire dati e informazioni e trasmettere documenti agli uffici doganali veritieri, completi e corretti;
d) effettuare con tempestività e correttezza gli adempimenti doganali, ivi compresi la trasmissione di dichiarazioni e comunicazioni, la liquidazione ed il versamento dei diritti doganali, imposte e tasse previsti dalla normativa doganale vigente;
e) conservare ordinatamente ed aggiornare all'occorrenza la documentazione doganale e l'elenco dei fornitori e degli spedizionieri doganali;
f) selezionare i fornitori e gli spedizionieri doganali con attenzione, in base ai requisiti di professionalità e onorabilità e improntare i rapporti con gli stessi alla massima correttezza e trasparenza.

I Destinatari del presente Modello devono inoltre astenersi dal:

g) predisporre, comunicare, o presentare all'Agenzia Doganale documentazioni o dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà riguardo ai prodotti oggetti di import/export;
h) omettere di comunicare, ovvero alterare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo ai prodotti oggetto di importazione e/o esportazione;
i) tenere comportamenti volti ad impedire od ostacolare, mediante l'occultamento di prodotti ovvero la distruzione di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo da parte delle Autorità Doganali.

Le disposizioni di cui alla presente Parte Speciale si applicano altresì ai Terzi eventualmente incaricati dalla Società dell'esecuzione degli adempimenti doganali (quali, ad esempio, spedizionieri e/o broker doganali).

Le responsabilità operative e di controllo sono ripartite, in particolare tra:

Sales Manager: raccolta dati della controparte, segnalazione red flags, divieto di formalizzare offerte/ordini prima delle verifiche;

Export Officer: verifiche soggettive, oggettive e geografiche; gestione autorizzazioni; tenuta delle evidenze;

Procurement: qualifica fornitori e verifica restrizioni;

Finance & Administration: controllo documentale e tracciabilità dei flussi finanziari;

Logistica/Delivery: spedizione solo previo nulla osta e verifica autorizzazioni;

Trade Compliance Officer: supervisione di secondo livello, aggiornamento normativo, controlli campionari e rapporti con OdV.

5. Protocolli specifici di comportamento

Ad integrazione ed ai fini di fornire un dettaglio operativo rispetto ai principi di comportamento declinati nel Codice Etico e nel presente Modello, AXIANS ha implementato le seguenti procedure:

- PMOG06_Procedura Gestione Import/Export, adempimenti doganali;
- PRO14_Gestione della logistica e del magazzino.

La procedura adottata dalla Società prevede come controlli:

A. La verifica soggettiva delle controparti

B. La verifica oggettiva del prodotto/servizio

C. La verifica geografica

D. La verifica dell'end use e dell'end user

E. L'escalation – in presenza di red flags o dubbi interpretativi

Si prevedono, inoltre, i seguenti principi specifici di comportamento.

A. Gestione delle importazioni

In relazione alle attività di importazione, è necessario:

- mantenere aggiornata l'anagrafica degli spedizionieri e dei fornitori;

- effettuare puntuali verifiche su spedizionieri e fornitori, con particolare riguardo ai requisiti di serietà ed affidabilità;
- codificare i fornitori extra-UE attraverso l'acquisizione della documentazione obbligatoria per l'anagrafica degli stessi, attestante la regolare costituzione della società nel paese di origine;
- verificare la completezza e la coerenza dell'ordine ai fornitori extra UE rispetto alla classificazione doganale (qualità della merce), al volume complessivo (quantità) e alla descrizione dell'articolo;
- verificare la correttezza del flusso logistico e di trasporto, unitamente ai connessi adempimenti doganali e fiscali. In ragione della modalità di trasporto, occorre impostare il flusso di approvvigionamento avendo cura di allocare oneri e responsabilità doganali e di trasporto (*Incoterms*) secondo procedure rispettose delle regole sulla movimentazione delle merci (es. ricorso a soggetti qualificati, doganalisti, luoghi approvati ed utilizzo spazi doganali autorizzati);
- controllare la ragionevolezza e la congruità dell'operazione/acquisto rispetto al valore di mercato medio comunemente applicato ed, eventualmente, la sussistenza di valide ragioni che giustifichino l'eventuale acquisto di merce c.d. "sottocosto";
- garantire la tracciabilità delle operazioni sino alla conferma dell'ordine al fornitore, attraverso l'utilizzo del *tool* informatico aziendale;
- verificare che l'incarico sia conferito a spedizionieri doganali di consolidata affidabilità (anche finanziaria);
- acquisire la fattura e ogni altra documentazione commerciale necessaria ad attestare la quantità della merce (volumi, peso, cubaggio), nonché la relativa origine doganale (certificato doganale d'origine o numero iscrizione al REX) e la conformità in base alle direttive CE applicabili

alla specifica tipologia di prodotti (Certificazioni/Dichiarazione di conformità);

- verificare la completezza e correttezza della documentazione di cui sopra con riferimento al valore della transazione, alla quantità e alla conformità della merce;
- garantire allo spedizioniere doganale l'accesso a tutti i documenti originali di cui al punto precedente ai fini della dichiarazione doganale, come prevista dalla normativa vigente;
- ricorrere a modalità di pagamento della merce tracciabili, subordinando il pagamento stesso all'acquisizione e alla verifica della correttezza della documentazione inerente il processo in esame;
- al momento della ricezione della bolletta doganale, verificare la corrispondenza della bolletta con i dati presenti in fattura e del dazio con quanto fatturato dallo spedizioniere; in caso di discordanza attivarsi per la rettifica;
- verificare la congruità del valore economico dell'offerta in relazione alle prestazioni oggetto del contratto;
- provvedere alla puntuale e scrupolosa descrizione della natura della merce importata, nonché al calcolo puntuale dei dazi o dei diritti di confine, di volta in volta determinati sulla base della natura della merce, del valore riportato sulla fattura del fornitore e del costo del trasporto e/o dei servizi accessori contrattualmente previsti;
- provvedere alla corretta archiviazione di tutta la documentazione doganale e alla registrazione della fattura di acquisto in contabilità,
- rispettare gli indicatori in ordine alla potenziale esclusione delle misure restrittive all'esportazione/importazione e delle sanzioni (a mero titolo esemplificativo e non esaustivo: improvvisi cambiamenti nell'attività commerciale a seguito di emanazione di pacchetti sanzionatori, ricezione di documentazione imprecisa o falsa);
- Rispettare le procedure di controllo import-export esistenti;
- Seguire le procedure aziendali in materia di due diligence delle terze parti.

Inoltre, è fatto divieto di:

- tenere comportamenti tali da integrare le fattispecie previste dai reati in materia di violazione delle misure restrittive dell'Unione Europea;

- introdurre o esportare merci da Paesi o da persone giuridiche o fisiche oggetto di sanzioni dell'Unione Europea;

- costruire triangolazioni per eludere le sanzioni unionali.

La società inserisce clausole contrattuali con le controparti che prevedono specifici impegni al rispetto dei regimi sanzionatori e meccanismi di risoluzione automatica del rapporto in caso di loro violazione e chiedono alle controparti l'end user Statement.

La capogruppo ha implementato un tool chiamato "Temis", il cui account è gestito soltanto dall'AD e dalla head of legal del gruppo, con il quale è possibile effettuare verifiche ad ampio spettro rispetto al possesso dei requisiti dei partner commerciali, ad es. sulla proprietà, azionisti, chi sono i legali rappresentanti, eventuali sanzioni.

Considerata la delicatezza di questa materia, è stato anche costituito il c.d. export control tandem quale presidio specialistico. Tale organismo fornisce supporto e consulenza alle funzioni aziendali attraversi l'analisi di casi complessi, le valutazioni relative a sanzioni internazionali e regimi restrittivi, il supporto nella gestione delle autorizzazioni, le attività di sensibilizzazione e formazione del personale.

B. Gestione delle esportazioni

In relazione alle attività di vendita e commercializzazione dei prodotti AXIANS verso Paesi extra UE, si prevede che:

- deve essere mantenuta costantemente aggiornata l'anagrafica degli spedizionieri e dei clienti;
- i rapporti con gli spedizionieri devono essere regolati da appositi contratti scritti;
- gli spedizionieri e i clienti devono essere qualificati ed essere sottoposti a puntuali verifiche, con particolare riferimento alla serietà ed affidabilità degli stessi;
- particolare attenzione deve essere posta nei confronti degli acquirenti extra-UE, acquisendo la documentazione obbligatoria attestante la regolare costituzione della società nel paese di origine;
- è necessario verificare la completezza e la coerenza della richiesta dell'acquirente extra UE rispetto alla classificazione doganale (qualità della merce), al volume complessivo (quantità) e alla descrizione dell'articolo;
- deve essere verificata la correttezza del flusso logistico e di trasporto, unitamente ai connessi adempimenti doganali e fiscali;
- in caso di introduzione di un nuovo *broker* doganale, sia richiesto allo spedizioniere l'inoltro della pre-bolla;
- occorre sempre verificare che i beni siano arrivati a destinazione dall'acquirente nel Paese terzo indicato nei documenti doganali e di trasporto;
- tutta la documentazione relativa alle esportazioni (*packing list*, documento DAU, documento DAE, ecc.) consegnata dal *broker* doganale che segue l'operazione deve essere raccolta all'interno del *dossier* di ciascuna commessa e conservata per un periodo di 10 anni;
- occorre verificare che tutti i documenti a supporto delle registrazioni, degli adempimenti e delle comunicazioni con le Autorità Doganali siano veritieri, autorizzati e conservati, per i periodi stabiliti dalla legislazione vigente, in modo ordinato e tale da poter effettuare verifiche sugli stessi in qualsiasi momento*;*
- Chiedere ai propri clienti adeguata documentazione che certifichi la non esportazione verso Paesi sensibili;
- rispettare gli indicatori in ordine alla potenziale esclusione delle misure restrittive all'esportazione/importazione e delle sanzioni (a mero titolo esemplificativo e non esaustivo: improvvisi cambiamenti nell'attività commerciale a seguito di emanazione di pacchetti sanzionatori, ricezione di documentazione imprecisa o falsa);
- valutare la coerenza della transazione commerciale e la conoscibilità del soggetto end-user;
- Rispettare le procedure di controllo import-export esistenti;
- Seguire le procedure aziendali in materia di due diligence delle terze parti.

C. Gestione degli adempimenti doganali

In relazione a tale area sensibile, AIXIANS garantisce che:

- sia verificata e approvata la documentazione da trasmettere alle autorità doganali ai fini dell'adempimento dei diritti di confine;
- siano notificate e comunicate eventuali irregolarità alle autorità competenti;
- sia verificata la redazione e la correttezza dei dati indicati nelle dichiarazioni doganali;
- siano mappati e identificati tutti gli acquisti effettuati da fornitori extra UE, con l'indicazione dei termini di trasporto/contratto utilizzati (*Incoterms*);
- siano stabilite le modalità di raccolta, verifica e approvazione della documentazione da trasmettere alle autorità doganali ai fini della restituzione/rimborso dei diritti doganali.

D. Gestione del magazzino

Con riferimento a tale processo sensibile, si rimanda ai protocolli di cui alla **Parte Speciale 10**.

6. Reporting all'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di verificare la corretta applicazione dei protocolli di cui alla presente Parte Speciale, i Responsabili delle Funzioni coinvolte nella gestione dei processi sensibili di cui al punto 2) dovranno trasmettere all'OdV le informazioni e le segnalazioni previste dalle procedure "*PMOG02 ODV Procedura Flussi informativi*" e "*PMOG01 Procedura Segnalazione Violazioni Whistleblowing*".