_Italia

AXIANS SAIV S.P.A.

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO EX D.LGS 231/01 – PARTI SPECIALI

AXIANS SAIV SpA con Socio Unico - Via Zamenhof, 843 - 36100 Vicenza - Italia
Tel: +39 0444 587500 - Fax: +39 0444 587501
www.axians.it

AXIANS SAIV S.P.A.

Modello di organizzazione gestione e controllo ex d.lgs 231/01 – parte speciale 1

Reati contro la Pubblica Amministrazione

I rapporti con la PA possono riguardare l'ottenimento di autorizzazioni, licenze, concessioni, finanziamenti pubblici, erogazioni, gare d'appalto ecc. ed è in questo ambito di rapporti e svolgimento di funzioni che si collocano le varie fattispecie di reato che gli enti possono commettere. La presente Parte Speciale si riferisce ai reati realizzabili nell'ambito dei rapporti tra la società e la P.A. In considerazione dell'analisi 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.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano, di altri enti pubblici o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi di pubblico interesse cui erano destinate. Tenuto conto che il momento di consumazione del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che non vengano destinati alle finalità per cui erano stati erogati.

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

Tale ipotesi di reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute –si ottengano, per sé o per altri e senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione europea. In questo caso, non rileva il corretto utilizzo delle erogazioni (come invece previsto dall'art. 316-bis), poiché il reato si concretizza nel momento stesso dell'ottenimento dei finanziamenti in modo indebito. Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie dell'art. 640-bis c.p., con riferimento a quei casi in cui la condotta non integri gli estremi più gravi della truffa ai danni dello Stato.

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

La fattispecie di cui all'art. 640 c.p. prevede un reato comune che può essere commesso da chiunque. Il fatto che costituisce reato consiste nel procurare a sé o ad altri un ingiusto profitto a danno di un altro soggetto, inducendo taluno in errore mediante artifici o raggiri. In particolare, nella fattispecie richiamata dall'art. 24 del D.Lgs. 231/2001 (i.e. art. 640 comma 2, n. 1 c.p.), rilevano i fatti commessi a danno dello Stato o di altro ente pubblico.

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

Tale ipotesi di reato si configura nel caso in cui la truffa (di cui all'art. 640 c.p.) sia posta in essere per conseguire indebitamente, contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

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

Questa fattispecie si realizza quando un soggetto, alterando in qualsiasi modo il funzionamento di un

sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. Tale ipotesi risulta aggravata se la frode informatica è commessa a danno dello Stato o di un altro ente pubblico ovvero se il fatto è commesso con abuso della qualità di operatore di sistema.

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

L'ipotesi di reato di cui all'art. 318 c.p. si configura nel caso in cui un pubblico ufficiale, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.

• Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.) e circostanze aggravanti (art. 319 bis c.p.)

Questa fattispecie si realizza quando un Pubblico Ufficiale, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro o altra utilità, o ne accetta la promessa. Ai sensi dell'art. 320 c.p. ("Corruzione di persona incaricata di un pubblico servizio"), le disposizioni di cui all'art. 318 e all'art. 319 si applicano anche alla persona incaricata di un pubblico servizio, qualora rivesta la qualità di pubblico impiegato. In entrambi i casi la pena è ridotta in misura non superiore a un terzo.

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

Questa fattispecie si realizza nei casi di comportamenti finalizzati alla corruzione commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

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

Questa fattispecie si realizza quando un Pubblico Ufficiale o l'incaricato di un pubblico servizio induce taluno a dare o promettere indebitamente, a lui o ad un terzo, denaro o altra utilità. La norma sanziona anche colui che dà o promette l'utilità.

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

Le pene stabilite nel primo comma dell'articolo 318, nell'art. 319, nell'art. 319-bis, nell'articolo 319- ter e Parte Speciale 1 - Reati nei rapporti con la Pubblica Amministrazione 4 nell'art. 320 c.p. in relazione alle suddette ipotesi degli artt. 318 e 319 c.p., si applicano anche a chi (i.e. corruttore) dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio denaro o altra utilità.

• Istigazione alla corruzione (art. 322 c.p.) e Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis)

Questa fattispecie si realizza nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, un Pubblico Ufficiale o un incaricato di pubblico servizio rifiuti l'offerta illecitamente avanzatagli. Ai fini dell'applicazione dei reati sopra elencati, ai pubblici ufficiali ed agli incaricati di pubblico servizio vanno equiparati, in forza del disposto di cui all'art 322-bis ("Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri") del codice penale, i membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri.

• Traffico illecito di influenze (art. 346-bis c.p.)

Chiunque, fuori dei casi di concorso nei reati di cui agli articoli 318, 319, 319 ter(2) e nei reati di corruzione di cui all'articolo 322 bis, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322 bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322 bis, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri, è punito con la pena della reclusione da un anno a quattro anni e sei mesi.

La stessa pena si applica a chi indebitamente dà o promette denaro o altra utilità.

La pena è aumentata se il soggetto che indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità riveste la qualifica di pubblico ufficiale o di incaricato di un pubblico servizio.

2. Processi sensibili, soggetti destinatari e obiettivi delle disposizioni contenute nella Parte Speciale -1-

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 principali processi sensibili ritenuti più specificatamente a rischio, sono i seguenti:

- la gestione dei rapporti e degli adempimenti verso la Pubblica Amministrazione, quali a titolo esemplificativo:

- la gestione degli adempimenti in materia tributaria;
- la gestione del contenzioso giudiziale o amministrativo;
- la gestione degli adempimenti di legge in materia di trattamenti previdenziali ed assistenziali del personale dipendente;
- la gestione degli adempimenti in materia di salute, sicurezza, igiene degli impianti e dei luoghi di lavoro;

- gestione dei rapporti con i funzionari pubblici degli Enti competenti in materia fiscale, sanitaria, di sicurezza pubblica, etc;
- la gestione dei rapporti con gli altri enti pubblici per l'ottenimento di autorizzazioni, licenze, provvedimenti amministrativi e permessi necessari per l'esercizio delle attività aziendali;
- la gestione delle ispezioni (amministrative, fiscali, previdenziali, in materia antinfortunistica ecc.);

- l'approvvigionamento di beni, servizi e prestazioni;
- l'assegnazione di incarichi di consulenze esterne;
- la gestione dei rapporti con agenti e intermediari;
- la gestione degli investimenti immobiliari e degli acquisti connessi;
- la gestione di incassi e pagamenti e la gestione della tesoreria;
- la gestione dei rimborsi spese a dipendenti e collaboratori;
- la gestione e la concessione di omaggi e liberalità;
- la richiesta e la gestione di finanziamenti, con particolare riferimento a quelli pubblici;
- la gestione delle assunzioni del personale dipendente e parasubordinato;
- la gestione di promozioni, avanzamenti di carriera, aumenti, assegnazione di "fringe benefits" a favore di dipendenti.

Le disposizioni della presente Parte Speciale hanno per destinatari tutti i soggetti coinvolti nei processi sopra identificati affinché gli stessi adottino regole di comportamento conformi a quanto prescritto al fine di prevenire il verificarsi dei reati ivi considerati. Nello specifico, la presente Parte Speciale ha lo scopo di:

a) indicare le procedure che i collaboratori di AXIANS sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, e ai responsabili delle funzioni aziendali che cooperano con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

3. Principi generali di comportamento

I seguenti divieti di carattere generale si applicano agli organi sociali, ai dirigenti e ai dipendenti di AXIANS in via diretta mentre ai consulenti, ai fornitori e ai partner in forza di apposite clausole contrattuali. Ai suddetti soggetti è fatto divieto di porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali 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); sono altresì proibite le violazioni ai principi ed alle procedure aziendali indicate nella presente Parte Speciale. Conformemente a quanto previsto nel Codice Etico, nel Codice di Condotta Anticorruzione, nelle procedure e nelle norme aziendali, ai soggetti sopra individuati è fatto divieto di:

a) effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri;

b) 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 seguendo quanto previsto nella procedura PMPOG03 relativamente ad omaggi, liberalità, sponsorizzazioni ed ospitalità;

c) ricorrere a forme diverse di aiuti o contribuzioni che, sotto veste di sponsorizzazioni, incarichi, consulenze o pubblicità abbiano invece le stesse finalità sopra vietate;

d) accordare vantaggi di qualsiasi natura (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);

e) 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;

f) 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;

g) effettuare prestazioni in favore dei consulenti e dei partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;

h) 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;

i) creare fondi a fronte di beni/servizi contrattualizzati a prezzi superiori a quelli di mercato oppure di fatturazioni inesistenti in tutto o in parte;

j) 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

k) 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;

l) presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;

m) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;

n) alterare e/o utilizzare abusivamente e in modo improprio i sistemi informatici aziendali.

4. Regole specifiche di condotta

Ad integrazione ed ai fini di fornire un dettaglio operativo rispetto ai principi già declinati nel Codice Etico e nel Codice di Condotta Anticorruzione, sono state formalizzate specifiche procedure e norme aziendali (vedi anche doc. 04 Disposizioni relative ai processi sensibili) aventi ad oggetto:

• la gestione degli adempimenti verso la Pubblica Amministrazione ;

• l'approvvigionamento di beni e prestazioni;

• la gestione e la concessione di omaggi e liberalità;

• la selezione, assunzione e gestione del personale;

• la gestione degli investimenti immobiliari e degli acquisti connessi;

• la gestione dei magazzini e dei cespiti;

• la gestione delle carte di credito aziendali e dei rimborsi delle spese viaggio;

• la gestione della tesoreria;

Nello svolgimento delle attività sensibili e/o strumentali, tutti i Destinatari del Modello, ed in particolare i soggetti aziendali coinvolti nelle aree a rischio, sono tenuti a tenere un comportamento corretto e trasparente, in conformità a quanto disposto dalle previsioni di legge esistenti in materia, dal Codice Etico adottato dalla Società e dalle procedure e norme aziendali sopra richiamate.

5. I controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività connesse ai Processi Sensibili al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello. A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo nonché libero accesso a tutta la documentazione aziendale rilevante. L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute. I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "PMOG02_ODV_Gestione Flussi informativi" e

“PMOG01_ODV_Protocollo whistleblowing” cui si rimanda.

AXIANS SAIV S.p.A.

Modello di organizzazione, gestione e controllo (ai sensi del D. Lgs. 8 giugno 2001 n. 231)

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

1. Le fattispecie dei reati di omicidio e lesioni colpose (art. 25 septies del D.Lgs. 231/2001)

La legge n. 123 del 3 agosto 2007 ha dettato nuove misure in materia di tutela della salute e della sicurezza sui luoghi di lavoro. Tra le principali novità è intervenuta la modifica del D. Lgs. n. 231/2001 ai sensi dell'articolo 9 della citata Legge 123 relativamente all'estensione della responsabilità amministrativa degli enti per gli illeciti commessi con la violazione di norme di salute e sicurezza e antinfortunistiche nei luoghi di lavoro. Il legislatore ha ritenuto di inserire l'articolo 25 septies che fa riferimento ai reati di cui agli artt. 589 c.p. (omicidio colposo) e 590 terzo comma c.p. (lesioni personali colpose gravi o gravissime), commessi con la violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati:

• Omicidio colposo (art. 589 c.p.)

La condotta punita dalla presente fattispecie di reato si concretizza in quei comportamenti che, violando le norme dettate ai fini della prevenzione degli infortuni sul lavoro e della tutela dell'igiene e della salute sui luoghi di lavoro, cagionano il decesso di una persona.

• Lesioni personali colpose gravi o gravissime (art. 590 c.p.)

Il reato si configura nel caso in cui per colpa si cagionino ad una persona lesioni gravi o gravissime, a seguito della violazione delle norme per la prevenzione degli infortuni sul lavoro. Le lesioni si considerano gravi nel caso in cui:

a) dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;

b) il fatto produce l'indebolimento permanente di un senso o di un organo (art. 583, comma 1, c.p.).

Le lesioni si considerano gravissime se dal fatto deriva:

a) una malattia certamente o probabilmente insanabile;

b) la perdita di un senso;

c) la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella;

d) la deformazione, ovvero lo sfregio permanente del viso (art. 583, comma 2, c.p.).

Ai fini della integrazione dei suddetti reati, non è richiesto l'elemento soggettivo del dolo, ovvero la coscienza e la volontà di cagionare l'evento lesivo, ma la mera negligenza, impudenza o imperizia del soggetto agente, ovvero l'inosservanza da parte di quest'ultimo di leggi, regolamenti, ordini o discipline (art. 43 c.p.).

2. Processi sensibili, soggetti destinatari e obiettivi delle disposizioni contenute nella Parte Speciale -2-

Le norme antinfortunistiche e di tutela dell'igiene e della salute sul lavoro hanno come destinatari alcuni specifici soggetti e cioè il datore di lavoro, i dirigenti, i preposti ed i lavoratori; alcune specifiche disposizioni riguardano il responsabile del servizio di prevenzione e protezione ed il rappresentante per la sicurezza; in tema di cantieri temporanei mobili alcune specifiche disposizioni riguardano ancora il committente, il responsabile dei lavori ed i coordinatori per la sicurezza. I reati di omicidio e di lesioni colpose commessi in violazione delle norme antinfortunistiche e di tutela dell'igiene e della salute sul lavoro interessano, a diverso titolo secondo le attribuzioni, i compiti e/o le responsabilità assegnate, principalmente i soggetti in questione.

Con riferimento ai reati ex art. 25 septies, i processi sensibili ritenuti teoricamente a rischio, sono i seguenti:

• la gestione degli adempimenti in materia di salute e sicurezza degli impianti e dei luoghi di lavoro;

• la gestione degli adempimenti in materia di salute e sicurezza presso le filiali.

A tal fine è stato predisposto il documento di valutazione dei rischi 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.

E' stato inoltre predisposto un organigramma societario con il quale sono stati definiti i ruoli secondo una struttura gerarchica disciplinata da un sistema di procure e deleghe.

AXIANS 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 previsti dalla legislazione.

L'attività appaltata ad aziende esterne è seguita con particolare attenzione; questi devono essere scelti in ragione della loro comprovata capacità e devono essere sensibilizzati ad operare mediante la puntuale osservanza delle norme che disciplinano la materia oggetto del presente capitolo.

3. Principi generali di comportamento

Le seguenti disposizioni di carattere generale si applicano al datore di lavoro, ai dirigenti, ai preposti, ai lavoratori, al responsabile del servizio di prevenzione e protezione, al rappresentante per la sicurezza, al R.S.G, al committente, al responsabile dei lavori, ai coordinatori per la sicurezza che sono organici in via diretta mentre ai consulenti, ai fornitori e ai partner in forza di apposite clausole contrattuali.

In particolare il Datore di Lavoro e tutti i soggetti aventi compiti, attribuzioni e/o responsabilità nella gestione degli adempimenti previsti delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, quali, a titolo esemplificativo, Responsabile del Servizio di Prevenzione e Protezione (R.S.P.P.), Addetti al Servizio di Prevenzione e Protezione (A.S.P.P.), Rappresentante dei Lavoratori per la Sicurezza (R.L.S.), Medico Competente (M.C.), Responsabile Sistema di Gestione della Sicurezza (R.S.G.S.), addetti al primo soccorso, addetti emergenze in caso d'incendio, 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, 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 "quasi incidenti";

d) l'idoneità delle risorse, umane - in termini di numero e qualifiche professionali, formazione - e materiali, 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.

In generale tutti i soggetti sopra individuati devono rispettare gli obblighi previsti dal D.lgs. 81/2008 ("Testo Unico sulla Sicurezza") e dalla normativa vigente in materia di salute e sicurezza sul lavoro – così come anche modificati dal nuovo Testo Unico sulla Sicurezza - nonché quanto definito 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 "quasi incidenti"), incidenti (indipendentemente dalla loro gravità) e violazioni alle regole di comportamento e alle procedure aziendali.

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

f) 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);

g) porre in essere o dare causa a violazioni dei principi comportamentali e delle procedure aziendali.

4. Regole specifiche di condotta

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

Nello svolgimento delle attività sensibili e/o strumentali, tutti i Destinatari del Modello, ed in particolare i soggetti aziendali coinvolti nelle aree a rischio, sono tenuti a tenere un comportamento corretto e trasparente, in conformità a quanto disposto dalle previsioni di legge esistenti in materia, dal Codice Etico adottato dalla Società e dalle procedure e norme aziendali sopra richiamate.

5. I controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività connesse ai Processi Sensibili al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello. A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo nonché libero accesso a tutta la documentazione aziendale rilevante. L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute. I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "PMOG02_ODV_Gestione Flussi informativi" e "PMOG01_ODV_Protocollo whistleblowing" cui si rimanda.

AXIANS SAIV S.P.A.

Modello di organizzazione gestione e controllo ex d.lgs 231/01 – parte speciale 3

Reati Societari

1. Le fattispecie dei reati societari e di market abuse (art. 25 ter e art. 25 sexies del D. Lgs. 231/2001)

La presente Parte Speciale si riferisce ai reati societari e ai reati di market abuse.
In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di AXIANS i seguenti reati:

• False comunicazioni sociali (artt. 2621 c.c.)

Questa fattispecie si realizza quando gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da uno a cinque anni.

• Impedito controllo (art. 2625 c.c.)

Questa fattispecie si realizza quando gli amministratori, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, ovvero alle società di revisione.

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

Questa fattispecie si realizza quando gli amministratori, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli.

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

Questa fattispecie si realizza quando gli amministratori ripartiscono utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite. La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

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

Questa fattispecie si realizza quando gli amministratori, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali anche della società controllante, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge. Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

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

Questa fattispecie si realizza quando gli amministratori, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzione del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori. Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

• Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.)

Questa fattispecie, introdotta con la L. n. 262 del 2005 si realizza quando l'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, della legge 12 agosto 1982, n. 576, o del decreto legislativo 21 aprile 1993, n. 124, viola gli obblighi previsti dall'articolo 2391, primo comma, e cioè omette di comunicare l'interesse che, per conto proprio o di terzi, abbia in una determinata operazione.

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

Questa fattispecie si realizza quando gli amministratori e i soci conferenti, anche in parte, formano o aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore l'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.

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

Questa fattispecie si realizza quando i liquidatori, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori. Il risarcimento del danno ai creditori prima del giudizio estingue il reato.

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

Questa fattispecie si realizza quando un soggetto, con atti simulati o fraudolenti, determina la maggioranza in assemblea allo scopo di procurare a sé o ad altri un ingiusto profitto.

• Aggiotaggio (art. 2637c.c.)

Questa fattispecie si realizza quando un soggetto diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

• Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza (art. 2638 c.c.)

Questa fattispecie si realizza quando gli amministratori, i direttori generali, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle Autorità Pubbliche di Vigilanza, o tenuti ad obblighi nei loro confronti, nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare le funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte, fatti che avrebbero dovuto comunicare, concernenti la situazione medesima. Tale fattispecie si realizza anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi. Parimenti vengono perseguiti gli amministratori, i direttori generali, i sindaci e i liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle Autorità Pubbliche di Vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette Autorità, consapevolmente ne ostacolino le funzioni.

• Abuso di informazioni privilegiate (art. 184 D.Lgs. n. 58 del 1998)

Questa fattispecie, introdotta con la L. n. 62 del 2005 si realizza quando chiunque, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime;

b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio;

c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a).

• Corruzione tra privati (art. 2635 cc)

Questa fattispecie si configura quando gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni. Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo.

Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.

Chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma, è punito con le pene ivi previste.

2. Processi sensibili, soggetti destinatari e obiettivi delle disposizioni contenute nella Parte Speciale – 3.

I reati previsti dall'art 25 ter e dell'art. 25 sexies del D.Lgs 231/2001 sono configurabili nell'ambito dei rapporti che intervengono tra la società, gli organi amministrativi e di controllo, i soci e i creditori, nonchè le Autorità Pubbliche di Vigilanza.

Con riferimento a tali reati i principali processi sensibili ritenuti più specificatamente a rischio sono i seguenti:

• la tenuta della contabilità e la gestione delle attività concernenti il processo di redazione del bilancio annuale e delle situazioni contabili infra-annuali;

• la gestione della tesoreria;

o la gestione e comunicazione di dati/notizie/strategie della società verso l'esterno;

o la predisposizione delle comunicazioni a soci e/o a terzi relative alla situazione economica, patrimoniale e finanziaria della società;

• la gestione dei rapporti e degli adempimenti verso Soci, Sindaci e organismi di controllo;

• la gestione delle operazioni straordinarie;

• la gestione delle operazioni con parti correlate.

Le disposizioni della presente Parte Speciale hanno per destinatari tutti i soggetti coinvolti nei processi sopra identificati affinché gli stessi adottino regole di condotta conformi a quanto prescritto al fine di impedire il verificarsi dei reati ivi considerati.

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

a) indicare le procedure che i collaboratori di AXIANS sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, e ai responsabili delle funzioni aziendali che con lo stesso cooperano, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

3. Principi generali di comportamento

I seguenti divieti di carattere generale si applicano agli organi sociali, ai dirigenti e ai dipendenti di AXIANS in via diretta mentre ai consulenti, ai fornitori e ai partner in forza di apposite clausole contrattuali.

Ai suddetti soggetti è fatto divieto di porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 ter e art. 25 sexies del D.Lgs. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.
Conformemente a quanto previsto nel Codice Etico, nelle procedure e nelle norme aziendali, i soggetti sopra individuati dovranno:

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

b) attivarsi affinché i fatti di gestione siano rappresentati correttamente e tempestivamente nella contabilità;

c) garantire la tempestività, l'accuratezza e il rispetto del principio di competenza nell'effettuazione delle registrazioni contabili;

e) assicurarsi che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima e coerente con la documentazione di supporto in modo da consentire la ricostruzione accurata dell'operazione;

f) assicurare il rispetto dei principi contabili adottati e la tracciabilità nelle scritture di chiusura, assestamento e rettifica e le poste estimative/valutative;

g) assicurare la corretta contabilizzazione delle operazioni di acquisto, cessione / dismissione di immobilizzazioni immateriali, materiali e finanziarie e relative plusvalenze o svalutazioni;

h) applicare adeguate procedure di controllo in caso di sopravvenienze attive apparentemente non giustificate o in caso di registrazioni di incassi (e pagamenti) di cui non si riscontri una contropartita di credito (o debito) corrispondente;

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

k) assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;

l) assicurare che i rapporti con i funzionari delle Autorità di Vigilanza siano gestiti esclusivamente dai soggetti dotati di idonei poteri;

m) effettuare con tempestività, correttezza e buona fede tutte le comunicazioni nei confronti di Autorità di Vigilanza – siano esse previste dalla legge o richieste dall'Autorità stessa - evitando ogni comportamento che possa risultare di ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate;

n) dare notizia, da parte di ogni Amministratore, agli altri amministratori e al collegio sindacale di situazioni di conflitto di interessi relative a una determinata operazione, precisandone la natura, i termini, l'origine e la portata e astenersi dal partecipare alla relativa deliberazione.

o) assicurare che ogni tipo di operazione straordinaria sia condotta nel pieno rispetto delle norme di legge o dei regolamenti applicabili;

p) mantenere riservati i documenti e le informazioni acquisiti nello svolgimento dei propri compiti e, in particolare, assicurare che la circolazione interna e verso Terzi di documenti contenenti informazioni potenzialmente privilegiate sia soggetta ad ogni necessaria attenzione e cautela, onde evitare pregiudizi alla società e indebite divulgazioni;

q) non comunicare ad altri, se non per motivi d'ufficio, le informazioni potenzialmente privilegiate di cui si viene a conoscenza;

v) assicurare che il trattamento fiscale delle operazioni societarie e gestionali, e relativa contabilizzazione, sia in linea con la normativa fiscale applicabile e con le disposizioni correlate (Agenzia Entrate, MEF, etc.), e sia effettuata nel rispetto delle procedure interne (a titolo esemplificativo e non esaustivo: operazioni esenti IVA, gestione degli omaggi, capitalizzazione di cespiti e diritti pluriennali e relativi ammortamenti, dismissione di cespiti e diritti pluriennali, valorizzazione del magazzino, gestione dei fondi svalutazione e rischi, etc).

4. Regole specifiche di condotta

Ad integrazione ed ai fini di fornire un dettaglio operativo rispetto ai principi già declinati nel Codice Etico, sono state formalizzate specifiche procedure e norme aziendali aventi ad oggetto:

- la chiusura delle situazioni contabili annuali e infrannuali e la redazione dell'informativa contabile

Nello svolgimento delle attività sensibili e/o strumentali, tutti i Destinatari del Modello, ed in particolare i soggetti aziendali coinvolti nelle aree a rischio, sono tenuti a tenere un comportamento corretto e trasparente, in conformità a quanto disposto dalle previsioni di legge esistenti in materia, dal Codice e dalle procedure e norme aziendali sopra richiamate.

5. I controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività connesse ai Processi Sensibili al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello. A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo nonché libero accesso a tutta la documentazione aziendale rilevante. L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute. I dettagli in merito al

contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "PMOG02_ODV_Gestione Flussi informativi" e "PMOG01_ODV_Protocollo whistleblowing" cui si rimanda.

AXIANS SAIV S.P.A.

Modello di organizzazione, gestione e controllo (ai sensi del D. Lgs. 8 giugno 2001 n. 231)

PARTE SPECIALE -4-

Delitti informatici e trattamento illecito di dati

Le fattispecie dei reati di delitto informatico e trattamento illecito di dati (art. 24 bis del D.Lgs. 231/2001)

La legge 18.3.2008 n. 48, ha introdotto nel D.Lgs. 231/2001 il nuovo art. 24-bis, che estende alle società, ricorrendone i presupposti, la responsabilità amministrativa per i reati commessi tramite un illecito utilizzo di documenti informatici e/o di sistemi informatici. La natura informatica che qualifica questi reati può riguardare le modalità di realizzazione della condotta, il suo oggetto materiale, il bene giuridico tutelato o la natura dei mezzi di prova.

• per documento informatico si intende "la rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti" secondo quanto previsto dal Codice dell'Amministrazione Digitale ex D.Lgs. 82/2005;

• per sistema informatico si intende, secondo la Convenzione di Budapest, "qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma per elaboratore, compie un'elaborazione automatica di dati".

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili i seguenti reati contemplati nel D.Lgs. 231/2001 all'art. 24-bis:

• 491 bis c.p. : Documenti informatici

Tale norma, di portata generale, estende le sanzioni previste per le falsità degli atti pubblici e privati, alle falsità riguardanti, rispettivamente, un documento informatico pubblico o privato avente efficacia probatoria.

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

La norma punisce l'accesso non autorizzato ad un sistema informatico o telematico altrui, protetto da misure di sicurezza interne al medesimo, siano esse di tipo hardware o software. La condotta illecita può concretizzarsi sia in un'attività di "introduzione" che di "permanenza" abusiva nel sistema informatico o telematico del proprietario del medesimo. Il reato è aggravato, tra gli altri casi, se commesso da un soggetto che abusa della sua qualità di operatore del sistema informatico o telematico. Il reato in questione, ad esempio, contrasta il fenomeno dei c.d. "hackers", e cioè di quei soggetti che si introducono nei sistemi informatici altrui, attraverso le reti telematiche, aggirando le protezioni elettroniche create dai proprietari di tali sistemi per tutelarsi dagli accessi indesiderati.

• 615 quater c.p.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici La norma in esame, tutelando la riservatezza dei codici di accesso, punisce la condotta di chi si procura illecitamente codici, parole chiave o altri mezzi idonei per accedere ad un sistema informatico o telematico protetto da misure di sicurezza. Tra le condotte illecite tipizzate dalla norma rientrano anche le attività di diffusione, comunicazione o consegna a terzi dei predetti codici idonei all'accesso, nonché di

comunicazione di indicazioni o istruzioni idonee al predetto scopo. La norma sanziona solo le condotte prodromiche e preparatorie all'accesso abusivo al sistema informatico o telematico. Il reato, ad esempio, è integrato qualora un soggetto ceda illecitamente ad un terzo la propria password di accesso alle banche dati cui abitualmente si collega.

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

La norma sanziona quelle condotte abusive che si sostanziano nella diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico otelematico. L'ipotesi tipica è quella di creazione dei c.d. "programmi virus", che diffondendosi e riproducendosi minano la funzionalità dei sistemi ove riescano ad introdursi.

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

La norma a tutela la riservatezza delle comunicazioni, punisce le condotte di intercettazione, impedimento o interruzione delle comunicazioni telematiche, poste in essere all'insaputa del soggetto che trasmette la comunicazione. La formula normativa di "comunicazioni telematiche" si presta ad abbracciare qualunque forma e qualunque strumento di divulgazione, ivi compresa la stessa via telematica, e quindi anche la diffusione deltesto della comunicazione via Internet oattraverso qualsiasi altra rete. Il reato è aggravato, tra gli altri casi, se commesso da un soggetto che abusa della sua qualità di operatore del sistema informatico o telematico.

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

La norma in esame punisce la condotta di installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche, posta in essere al di fuori dei casi espressamente consentiti dalla legge.

• 635 ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità

La norma in questione al primo comma punisce le condotte prodromiche e preparatorie al danneggiamento di informazioni, dati e programmi informatici di cui all'art. 635 bis c.p. riguardanti informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità. La concreta realizzazione del danno, invece, integra un'autonoma ipotesi di reato, sanzionata più pesantemente nel comma 2 della norma in commento.

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

La norma in questione punisce i fatti di danneggiamento previsti dall'art. 635 quater c.p. riguardanti i sistemi informatici o telematici di pubblica utilità. Il reato è aggravato, tra gli altri casi, se commesso da

un soggetto che abusa della sua qualità di operatore del sistema informatico o telematico.

• 640 quinquies c.p. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica La norma in esame punisce la frode informatica commessa esclusivamente dal soggetto che presta servizi di certificazione di firma elettronica ovvero fornisce altri servizi connessi con quest'ultimo, secondo quanto previsto dal Codice dell'Amministrazione Digitale ex D.Lgs. 82/2005. La condotta punita penalmente consiste nella violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato: si tratta, in particolare, degli obblighi di controllo e garanzia previsti dal predetto D.Lgs. 82/2005.

2. Processi sensibili, soggetti destinatari e obiettivi delle disposizioni contenute nella Parte Speciale -4-

Con riferimento ai reati previsti dall'art. 24-bis i principali processi sensibili ritenuti più specificatamente a rischio, sono i seguenti:

• Gestione delle modifiche architetturali ed applicative

• Continuità del servizio

• Sicurezza logica dei sistemi

• Gestione del Service Desk e degli incidenti/problemi

• Misure per la sicurezza delle reti di trasmissione

• Gestione dell'ambiente fisico

Le disposizioni della Presente Parte Speciale hanno per destinatari tutti i soggetti aziendali coinvolti, a vario titolo, nella gestione o nell'utilizzo dei sistemi informativi aziendali; ovvero tutti i dipendenti, i collaboratori esterni, temporanei e continuativi, i fornitori che per le loro attività abbiano accesso fisico o logico ai sistemi informativi di AXIANS.

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

a) indicare le procedure che i collaboratori di AXIANS sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, e ai responsabili delle funzioni aziendali che con lo stesso cooperano, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

3. Principi generali dicomportamento

Conformemente a quanto previsto nel Codice Etico, nelle procedure e nelle norme aziendali, ai soggetti sopra individuati è fatto divieto di:

• porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di: o acquisire abusivamente informazioni contenute nei suddetti sistemi informativi;

- danneggiare, distruggere dati contenuti nei suddetti sistemi informativi;
- utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché o procedere alla diffusione degli stessi.

• porre in essere condotte miranti alla distruzione o all'alterazione dei documenti informatici aventi finalità probatoria in assenza di una specifica autorizzazione;

• utilizzare o installare programmi diversi da quelli autorizzati dal personale della Funzione Information Technology;

• aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (Antivirus, Firewall, proxy, server,…);

• lasciare il proprio Personal Computer sbloccato e incustodito;

• rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;

• detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;

• entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato.

Il personale della Funzione Information Technology deve attivarsi, in base al proprio ruolo e responsabilità, al fine di porre in essere quelle azioni necessarie per:

• verificare la sicurezza della rete e dei sistemi informativi aziendali;

• identificare le potenziali vulnerabilità nel sistema dei controlli IT;

• valutare la corretta implementazione tecnica del sistema "deleghe e poteri" aziendale a livello di sistemi informativi ed abilitazioni utente riconducibile ad una corretta segregazione dei compiti;

• vigilare sulla corretta applicazione di tutti gli accorgimenti ritenuti necessari al fine di fronteggiare,

nello specifico, i delitti informatici e di trattamento dei dati, suggerendo ogni più opportuno adeguamento.

I responsabili delle Direzioni/Funzioni devono attivarsi, in base al proprio ruolo e responsabilità, al fine di porre in essere le azioni necessarie per monitorare il corretto utilizzo degli accessi (user - id, password) ai sistemi informativi di terze parti. Tutti i soggetti inclusi nel presente documento sono tenuti a rispettare, per le attività di rispettiva competenza, le seguenti regole:

• gli strumenti aziendali devono essere utilizzati nel rispetto delle policy e procedure aziendali definite;

• le credenziali utente devono essere oggetto di verifica periodica al fine di prevenire eventuali erronee abilitazioni ai sistemi applicativi;

• 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 navigazione in internet e l'utilizzo della posta elettronica attraverso i sistemi informativi aziendali deve essere limitato alle sole attività lavorative;

• siano, sui diversi applicativi aziendali, applicate le regole atte ad assicurare l'aggiornamento delle password dei singoli utenti;

• la sicurezza fisica dell'infrastruttura tecnologica di AXIANS sia implementata nel rispetto delle regole interne ed in modo da consentire un monitoraggio delle attività di gestione e manutenzione sulla stessa;

• le attività svolte da parte di fornitori terzi in materia di:

- networking;
- gestione software applicativi;
- gestione sistemi hardware;

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).

3. Regole specifiche dicondotta

Ad integrazione ed ai fini di fornire un dettaglio operativo rispetto ai principi già declinati nel Codice Etico, sono state formalizzate specifiche policy, procedure e norme aziendali aventi ad oggetto:

• la sicurezza informatica;

• le modalità di utilizzo delle dotazioni informatiche;

• la gestione degli accessi logici e dei profili-utente;

• le modalità di gestione degli incidenti/problemi;

• le modalità di gestione dei dati personali nel rispetto della normativa vigente.

Nell'ambito del Sistema di Sicurezza delle Informazioni sono state definite le misure per la sicurezza delle reti di trasmissione, le misure di sicurezza fisica e logica nonché le procedure adottate per garantire la continuità del servizio.

Nello svolgimento delle attività sensibili e/o strumentali, tutti i Destinatari del Modello, ed in particolare i soggetti aziendali coinvolti nelle aree a rischio, sono tenuti a tenere un comportamento corretto e trasparente, in conformità a quanto disposto dalle previsioni di legge esistenti in materia, dal Codice Etico adottato dalla Società e dalle procedure e norme aziendali sopra richiamate.

5. I controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività connesse ai Processi Sensibili al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello. A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo nonché libero accesso a tutta la documentazione aziendale rilevante. L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute. I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "PMOG02_ODV_Gestione Flussi informativi" e "PMOG01_ODV_Protocollo whistleblowing" cui si rimanda.

AXIANS SAIV S.P.A.

Modello di organizzazione gestione e controllo ex d.lgs 231/01 – parte speciale 5

Corruzione tra privati

1. Il reato di "corruzione tra privati" [art. 25-ter c.1 lettera s-bis) del D.Lgs. 231/2001]

La legge 6 novembre 2012, n. 190, ha ampliato il catalogo dei reati presupposto del D.Lgs. n. 231/2001, prevedendo:
a) La fattispecie di "induzione indebita a dare o promettere utilità", di cui all'articolo 319- quater c.p. richiamato dall'art. 25, c. 3 del D.Lgs. 231/2001
b) La fattispecie di "corruzione tra privati", di cui all'articolo 2635 c.c., richiamato dall'art. 25-ter comma 1, lettera s-bis del D.Lgs. 231/2001. Con il D.Lgs. 38/2017 del 14 aprile 2017, l'ordinamento italiano ha revisionato il dettato dell'art. 2635 c.c. "corruzione tra privati". La nuova formulazione prevede, con riferimento alla corruzione "passiva":
a) che i destinatari della norma non siano più soltanto coloro che rivestono posizioni apicali all'interno delle società (amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili, sindaci e liquidatori), ma anche coloro che svolgono attività lavorativa con l'esercizio di funzioni direttive "di fatto";
b) la punibilità non solo per la "dazione e promessa", ma anche per la "sollecitazione" per sé o per altri di denaro o altra utilità non dovuti;
c) la punibilità delle suddette condotte anche se poste in essere da un intermediario ("per interposta persona");
d) la punibilità anche in assenza di un danno alla società o all'ente.

Con riferimento alla corruzione "attiva", si rende possibile la punibilità anche dell'offerta di denaro o altra utilità (e non solo della dazione e della promessa) anche nell'eventualità in cui sia posta in essere da un intermediario. Al contempo è stato introdotto l'art. 2635-bis c.c. "istigazione alla corruzione tra privati". Diviene punibile colui che cercherà di corrompere le figure di cui sopra, anche senza che la dazione, promessa o sollecitazione siano accettate.
In particolare, la norma prevede che chiunque offra o prometta denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.
Il reato presupposto è procedibile a querela della persona offesa, fatto salvo il caso in cui sia procedibile d'ufficio qualora dal fatto derivi una distorsione della concorrenza, intendendosi tali tutte quelle attività che abbiano per oggetto o fine quello di "impedire, restringere o falsare in maniera consistente il gioco della concorrenza" (art. 2 L. 287/90).

1. Processi sensibili, soggetti destinatari e obiettivi delle disposizioni contenute nella Parte Speciale -5-

Le condotte tipiche della corruzione nei rapporti con la Pubblica Amministrazione sono applicabili anche con riferimento al reato nei confronti di privati. Sono pertanto "sensibili" tutti i processi già considerati nella Parte Speciale 1, con particolare riferimento ai processi c.d. "strumentali", ovvero

laddove può concretizzarsi una modalità di comportamento che costituisce un mezzo per un evento corruttivo, anche successivo:

• l'approvvigionamento di beni e servizi e l'assegnazione di incarichi professionali;
• la gestione dei rapporti con agenti e intermediari;
• la gestione amministrativa del processo di vendita (ciclo attivo) e del processo di acquisto o di investimento (ciclo passivo);
• la gestione di incassi e pagamenti;
• la gestione dei rimborsi spese e delle spese di rappresentanza;
• la gestione e la concessione di omaggi, sponsorizzazioni e liberalità;
• la richiesta e la gestione di finanziamenti;
• la gestione delle assunzioni del personale dipendente e parasubordinato;
• la gestione di promozioni, avanzamenti di carriera, aumenti, assegnazione di "fringe benefits" a favore di dipendenti;

In aggiunta, sono da considerarsi "sensibili" ai fini del rischio di commissione del reato di corruzione tra privati tutte quelle attività aziendali nel cui ambito può manifestarsi l'occasione per la commissione del reato. Si ritengono dunque più specificatamente a rischio le seguenti attività:

• la gestione dei rapporti con le controparti contrattuali o con altre imprese, sebbene operanti in settori diversi;
• la gestione dei rapporti con le controparti bancarie e assicurative;
• la gestione dei rapporti con gli analisti finanziari e società di rating;
• l'ottenimento di certificazioni e gestione dei rapporti con enti certificatori.

Le disposizioni della presente Parte Speciale hanno per destinatari tutti i soggetti coinvolti nei processi sopra identificati affinché gli stessi adottino regole di condotta conformi a quanto prescritto al fine di prevenire il verificarsi dei delitti ivi considerati.

Nello specifico la presente Parte Speciale ha lo scopo di:

a) indicare i principi che i destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, ed ai Responsabili delle funzioni aziendali che con lo stesso cooperano, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

2. Principi generali di comportamento

I seguenti principi di carattere generale si applicano agli organi sociali, ai dirigenti ed ai dipendenti in via diretta, mentre al personale non dipendente e agli altri consulenti, ai fornitori e ai partner in forza di apposite clausole contrattuali.

Ai suddetti soggetti è fatto divieto di porre in essere, concorrere o dare causa alla realizzazione di azioni o di omissioni tali da integrare, direttamente o indirettamente, il reato di corruzione tra privati; sono altresì proibite le violazioni ai principi comportamentali e divieti previsti nella presente Parte Speciale, nel Codice Etico e nel Codice di Condotta Anticorruzione.

Conformemente a quanto previsto nei Codici sopra richiamati e nelle procedure e norme aziendali, i soggetti sopra individuati dovranno:

a) tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge, nonché delle procedure aziendali interne, in tutte le attività che comportano rapporti con altre Società, laddove AXIANS potrebbe ricavare un indebita utilità o interesse, concedendo o promettendo, anche per interposta persona, denaro, omaggi o altra utilità, nei rapporti con:

- amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci, liquidatori; o qualsiasi soggetto sottoposto alla direzione e alla vigilanza di uno di essi. Inoltre, ai soggetti sopra individuati è vietato, a mero titolo esemplificativo:

b) porre in essere o dare causa a violazioni dei protocolli specifici di comportamento e di controllo contenuti nella presente Parte Speciale, nonché della regolamentazione aziendale richiamata nel successivo paragrafo 4;

c) concedere o promettere denaro, altri tipi di omaggio, benefici o altra utilità a soggetti – come sopra menzionati – appartenenti a:

- controparti contrattuali, società o imprese concorrenti;

- controparti bancarie o assicurative, al fine di ottenere, ad esempio, estensioni di linee di fido, minori covenants o condizioni maggiormente contrattuali favorevoli;

- società di rating, al fine di ottenere giudizi particolarmente favorevoli;

- società di certificazione, al fine di ottenere la certificazione od il rinnovo della stessa, anche in assenza dei requisiti;

- “buyer” di clienti / potenziali clienti, nell’ambito di negoziazioni, al fine di ottenere

condizioni contrattuali maggiormente favorevoli per AXIANS;

- altri soggetti che rappresentino una società appaltante, affinché favoriscano la conclusione di una operazione a condizioni economiche favorevoli per AXIANS, oppure ostacolino una trattativa con altra società.

3. Regole specifiche di condotta

Ad integrazione dei principi comportamentali e dei divieti sopra elencati, oltre che alle previsioni del Codice Etico e del Codice di Condotta Anticorruzione, sono state formalizzate specifiche procedure interne e norme aziendali volte a disciplinare gestione dei ricavi

- gli investimenti ;
- la gestione di omaggi, sponsorizzazioni, liberalità ed ospitalità ;
- la gestione dei pagamenti e della tesoreria ;
- l'approvvigionamento di beni, servizi e prestazioni.

Nello svolgimento delle attività sensibili e/o strumentali, tutti i Destinatari del Modello, ed in particolare i soggetti aziendali coinvolti nelle aree a rischio, sono tenuti a tenere un comportamento corretto e trasparente, in conformità a quanto disposto dalle previsioni di legge esistenti in materia, dal Codice Etico e Codice di Condotta Anticorruzione adottati da AXIANS e dalla Società e dalle procedure e norme aziendali sopra richiamate.

5. I controlli dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività connesse ai Processi Sensibili al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello. A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo nonché libero accesso a tutta la documentazione aziendale rilevante. L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute. I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "PMOG02_ODV_Gestione Flussi informativi" e "PMOG01_ODV_Protocollo whistleblowing" cui si rimanda.