MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEGLI ARTT. 6 e 7 DEL D.LGS. 231/2001 E DELL'ART. 30 D.LGS. 81/2008

NUOVA EDIZIONE 2023

SAN MARCO S.P.A.

DATI SULL'AZIENDA

RAGIONE SOCIALE

SAN MARCO S.P.A.

DATI SULL'AZIENDA

Denominazione: SAN MARCO S.p.a.
Forma giuridica: SOCIETA' PER AZIONI
Sede legale:
Codice fiscale e Partita IVA:
Numero REA: -

SCOPO - OGGETTO SOCIALE

GLOSSARIO

• "CCNL": il Contratto Collettivo Nazionale di Lavoro (contratto dei dipendenti di imprese e società esercenti servizi ambientali) attualmente in vigore ed applicato da SAN MARCO ;
• "Organismo di Vigilanza" ("O.d.V."): organismo interno preposto alla vigilanza sul funzionamento e sull'osservanza del Modello e al relativo aggiornamento, di cui all'articolo 6, comma 1, lettera b) del D.Lgs. 231/01;
• "Dipendenti": tutti i dipendenti di SAN MARCO ;
• "Consulenti": coloro che agiscono in nome e/o per conto di SAN MARCO sulla base di un mandato o di altro rapporto di collaborazione;
• "Partner": controparti contrattuali di SAN MARCO , sia persone fisiche che giuridiche, con cui la società addivenga ad una qualunque forma di

collaborazione contrattualmente regolata (Associazione temporanea d'impresa - ATI, franchising, joint venture, consorzi, ecc.), ove destinati a cooperare con la Società nell'ambito dei Processi Sensibili;
• "Collaboratori": Amministratori, Dipendenti e Consulenti;
• "Terzi": clienti, collaboratori esterni e Partner;
• "D.Lgs. 231/01": il Decreto Legislativo n. 231 dell'8 giugno 2001 e successive modifiche ed integrazioni;
• "D.Lgs. 81/08": il Decreto Legislativo n. 81 del 9 Aprile 2008, entrato in vigore il 15 maggio 2008, recante il "Testo Unico in materia di tutela della salute e sicurezza sui luoghi di lavoro";
• "Linee Guida di Confindustria": le linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/01 emanate da Confindustria in data 3 novembre 2003 e successive integrazioni;
• "Modelli" o "Modello": i modelli o il modello di organizzazione, gestione e controllo previsti dal D.Lgs. 231/01;
• "Operazione Sensibile": operazione o atto che si colloca nell'ambito dei Processi Sensibili e può avere natura commerciale, finanziaria, di lobby tecnico-politica o societaria (quanto a quest'ultima categoria esempi ne sono: riduzioni di capitale, fusioni, scissioni, operazioni sulle azioni della società controllante, conferimenti, restituzioni ai soci, ecc.);
• "Organi Societari": Amministratore unico, Presidente;
• "P.A.": la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio;
• "Processi Sensibili": attività di SAN MARCO nel cui ambito ricorre il rischio di commissione dei Reati;
• "Reati": i reati previsti dal D.Lgs. 231/01;
• "SGQ": il sistema di gestione qualità interno proprio di SAN MARCO ;

PARTE GENERALE

Il Decreto Legislativo n. 231/01

In data 8 giugno 2001 è stato emanato - in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 - il D.Lgs. 231/01, entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali cui l'Italia ha già da tempo aderito.

Il D.Lgs. 231/01, recante la “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica” ha introdotto per la prima volta in Italia la responsabilità in sede penale degli enti (persone giuridiche o associazioni) per alcuni reati commessi nell'interesse o a vantaggio degli stessi, da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente (ad esempio, amministratori o altri dirigenti) o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso e, infine, da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati (ad esempio, dipendenti). Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto.

La nuova responsabilità introdotta dal D.Lgs. 231/01 mira a coinvolgere nella punizione di taluni illeciti penali gli enti che abbiano tratto un vantaggio dalla commissione dell'illecito. Per tutti gli illeciti commessi è sempre prevista l'applicazione di una sanzione pecuniaria; per i casi più gravi sono previste anche misure interdittive quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la P.A., l'interdizione dall'esercizio dell'attività, l'esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi.

Quanto ai reati cui si applica la disciplina in esame, si tratta attualmente delle seguenti tipologie, qui descritte in termini meramente riassuntivi:

1. delitti contro la pubblica amministrazione (quali corruzione e malversazione ai danni dello Stato, truffa ai danni dello Stato e frode informatica ai danni dello Stato, indicati agli artt. 24 e 25 del D.Lgs. 231/2001) o contro la fede pubblica (quali Falsita` in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, indicati all’art. 25-bis D.Lgs. 231/2001);
2. reati societari (quali false comunicazioni sociali, falso in prospetto, illecita influenza sull’assemblea, indicati all’art. 25-ter D.Lgs. 231/2001);

3. delitti in materia di terrorismo e di eversione dell'ordine democratico (ivi incluso il finanziamento ai suddetti fini), indicati all'art. 25-quater D.Lgs. 231/2001;
4. delitti contro la personalità individuale (quali lo sfruttamento della prostituzione, la pornografia minorile, la tratta di persone e la riduzione e mantenimento in schiavitù, indicati all'art. 25-quinquies D.Lgs. 231/2001);
5. Abusi di mercato, indicati dall'articolo 25-sexies D.Lgs. 231/2001);
6. Pratiche di mutilazione degli organi genitali femminili, indicati dall'art.25-quater 1. del Dlgs 231/2001);
7. Reati transnazionali: l'associazione per delinquere, di natura semplice e di tipo mafioso, l'associazione finalizzata al contrabbando di tabacchi lavorati esteri o al traffico illecito di sostanze stupefacenti o psicotrope, il riciclaggio, l'impiego di denaro, beni o altra utilità di provenienza illecita, il traffico di migranti ed alcuni reati di intralcio alla giustizia se rivestono carattere di transnazionalità;
8. Omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies D.Lgs. 231/2001);
9. reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita previsti dagli articoli 648, 648-bis e 648-ter del codice penale (art. 25-octies D.Lgs. 231/01);
10. Delitto di autoriciclaggio (art. 648 ter-1 D.lgsl 231/2001);
11. Delitti informatici ed illecito trattamento dei dati c.d. "Cybercrime" (art. 24-bis D.Lgs. 231/2001);
12. Delitti di criminalità organizzata (art. 24-ter D.Lgs. 231/01);
13. Delitti contro l'industria e il commercio (art. 25-bis-1 D.Lgs. 231/01);
14. Delitti in materia di violazioni del diritto d'autore (art. 25-nonies D.Lgs. 231/01);
15. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorita' giudiziaria (art. 25-decies D.Lgs. 231/01);
16. Reati ambientali ed inquinamento del mare da parte delle navi (art. 25-undecies);
17. Impiego di lavoratori stranieri irregolari (art. 25-duodecies);
18. Corruzione tra privati (art. 25-ter)

    La descrizione delle fattispecie rilevanti è contenuta nelle parti speciali del presente Modello alle quali si fa qui espresso rinvio.

L'ESIMENTE CONTEMPLATA DAGLI ARTT. 6 E 7 DEL D.LGS. 231/01

L'articolo 6 del D.Lgs. 231/01 introduce una particolare forma di esonero dalla responsabilità per gli eventuali reati commessi da soggetti apicali, qualora l'Ente dimostri:

a) di aver adottato ed efficacemente attuato attraverso il suo organo dirigente, prima della commissione del fatto, il Modello idoneo a prevenire reati della specie di quello verificatosi;

b) di aver affidato ad un organismo interno, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza dei Modelli, nonché di curare il loro aggiornamento;

c) che le persone che hanno commesso il reato hanno agito eludendo fraudolentemente i suddetti Modelli;

d) che non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lett. b).

L'art. 7 del D.Lgs. 231/01 prevede l'esonero da responsabilità per i reati commessi da soggetti sottoposti alla direzione dei vertici aziendali se questi ultimi non hanno violato i propri obblighi di direzione o vigilanza; tale violazione è comunque esclusa se l'Ente, prima della commissione del fatto, ha adottato ed efficacemente attuato attraverso il suo organo dirigente, il Modello idoneo a prevenire reati della specie di quello verificatosi.

Il D.Lgs. 231/01 prevede, inoltre, che – in relazione all'estensione dei poteri delegati ed al rischio di commissione dei reati – i Modelli debbano rispondere alle seguenti esigenze:

1. individuare le aree a rischio di commissione dei reati previsti dal Decreto;
2. predisporre specifici protocolli al fine di programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
3. prevedere modalità di individuazione e di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
4. prescrivere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
5. configurare un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Lo stesso Decreto dispone che i Modelli possono essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento (Linee Guida) redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni, osservazioni sulla idoneità delle Linee Guida a prevenire i reati (si veda Decreto del Ministero della Giustizia del 26 giugno 2003 n. 201).
È infine previsto che, negli enti di piccole dimensioni, il compito di vigilanza possa essere svolto direttamente dall'organo dirigente (art. 6, comma 4, D.Lgs. 231/01)

IL MODELLO ORGANIZZATIVO SECONDO LE DISPOSIZIONI DELL'ART. 30 DEL D.LGS. 81/08

La materia dei modelli organizzativi con efficacia esimente, e addirittura tutta la materia della compliance aziendale, è stata profondamente innovata con l'introduzione del D.Lgs. 81/08, recante il “Testo Unico in materia di tutela della salute e sicurezza nei luoghi di lavoro”.
Il D.lgs. 81/08 infatti stabilisce un nuovo regime per i modelli organizzativi, ponendo all'attenzione dei responsabili due importanti novità legislative.
In primo luogo il modello organizzativo non è più uno strumento di adozione facoltativa, bensì è obbligatorio per le materie di cui si occupa il Testo Unico: stabilisce infatti l'art. 30 del D.Lgs. 81/08 che il modello organizzativo “deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:
a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
d) alle attività di sorveglianza sanitaria;
e) alle attività di informazione e formazione dei lavoratori;
f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate”.
Il tenore letterale dell'art. 30 è del tutto inequivoco: il modello organizzativo **deve** essere adottato per creare gli strumenti aziendali idonei ad ottemperare agli obblighi di legge in materia di salute e sicurezza dei lavoratori. Resta salva la facoltatività del modello organizzativo per quanto riguarda le altre fattispecie di

reato contemplate nel D.Lgs. 231/01, che mantiene tutta la sua validità, quindi rimane assolutamente consigliabile l'adozione di un modello organizzativo omnicomprensivo, che contemperi ed assolva le esigenze di entrambe le norme in esame.
Tale operazione pone alcuni problemi pratici consistenti nella difficoltà di assolvere ad esigenze completamente diverse quali quelle di prevenzione di alcuni specifici reati e di ottemperanza all'obbligo di assicurare un ambiente di lavoro sano e sicuro.
SAN MARCO ha scelto di adottare un modello organizzativo unico, che assolva con precisione le richieste e gli obblighi posti sia dal D.Lgs. 81/08, sia dal D.Lgs. 231/01, affrontando e risolvendo i problemi applicativi posti nella pratica dalla necessità di far convivere due norme così diverse. Si ribadisce che sono in fase di implementazione tutti gli aspetti specifici relativi alla salute e sicurezza dei lavoratori.

La seconda innovazione portata dal Testo Unico riguarda la necessità di adeguare il modello organizzativo di adozione obbligatoria alle linee guida dei sistemi OHSAS 18001:2007 o alle linee guida UNI-INAIL. Nel sistema del D.lgs. 231/01 infatti non era previsto come necessario l'adeguamento ad una modalità predefinita di attuazione, ed era lasciata libertà di autodeterminazione agli enti, fermo restando il giudizio di idoneità del modello organizzativo, vero discrimine per attivare l'efficacia esimente della responsabilità dell'ente in caso di commissione di reati.
Oggi l'efficacia esimente viene presunta allorquando il Modello organizzativo sia conforme alle linee guida indicate, ed assolva alle esigenze di cui al comma 1 dell'art. 30 del D.Lgs. 231/01.

LE LINEE GUIDA DETTATE DA CONFINDUSTRIA

Come si diceva nel capitolo precedente, il D.Lgs. 231/01 ha disposto agli artt. 6 e 7 che l'adozione ed efficace attuazione di un modello organizzativo potesse avere efficacia esimente della responsabilità dell'ente in caso di commissione di un reato. Il Decreto tuttavia non ha disposto in alcun modo circa un riconoscimento a priori della idoneità di un modello organizzativo; le associazioni di categoria hanno però dettato alcune indicazioni per la realizzazione di un adeguato modello organizzativo. In particolare Confindustria ha predisposto le Linee Guida per la costruzione dei modelli organizzativi ex D.Lgs. 231/01 alle quali si è fatto riferimento per lo sviluppo del Modello di SAN MARCO , si è fatto inoltre riferimento alla best practice italiana esistente in materia, quali strumenti operativi e di indirizzo maggiormente confacenti alla struttura organizzativa della Società.
Gli strumenti individuati per la costruzione del Modello, i punti fondamentali per la costruzione dello stesso possono essere così sintetizzati:
- la risk analysis, ovvero individuazione delle aree di rischio, volta a verificare in quale area/settore aziendale sia possibile la realizzazione dei Reati;
- revisione e adattamento delle procedure aziendali in grado di prevenire i rischi attraverso l'adozione di apposite procedure;
- istituzione di un Organismo di Vigilanza, dotato di autonomi poteri di informazione e di controllo e di intervento correttivo.
Le componenti più rilevanti del modello organizzativo sono individuate nei seguenti elementi:
- codice etico;
- procedure manuali ed informatiche;
- Organismo di Vigilanza;
- comunicazione al personale e sua formazione.
Le componenti del sistema di controllo devono essere informate ai seguenti principi:
• verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
• applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);
• documentazione dei controlli;

• previsione di un adeguato sistema sanzionatorio per la violazione delle procedure previste dal Modello;
• individuazione dei requisiti dell'Organismo di Vigilanza, riassumibili in autonomia, indipendenza e professionalità;
• previsione di obblighi di informazione dell'Organismo di Vigilanza;
• possibilità, nell'ambito dei gruppi societari, di soluzioni organizzative che accentrino presso la capogruppo le funzioni previste dal D.Lgs. 231/01.

Resta inteso che la scelta di non adeguare il Modello ad alcune indicazioni di cui alle Linee Guida di Confindustria o alla best practice applicata, non inficia di per sé la validità dello stesso. Il singolo Modello, infatti, dovendo essere redatto con riferimento alla realtà concreta della Società, ben può discostarsi da tali indicazioni che, per loro natura, hanno carattere generale.

IL MODELLO ORGANIZZATIVO DI SAN MARCO

Funzione e scopo del Modello

SAN MARCO è sensibile alle aspettative degli stakeholders ed è consapevole del valore che agli stessi può derivare da un sistema di controllo interno idoneo a prevenire la commissione di Reati da parte dei propri Dipendenti, Amministratori, Consulenti e Partner.
Pertanto, l'adozione e l'efficace attuazione del Modello non solo consente alla società di beneficiare dell'esimente prevista dal D.Lgs. 231/01, ma migliora la sua Corporate Governance, limitando il rischio di commissione dei Reati.
Scopo del Modello è la predisposizione di un sistema strutturato ed organico di procedure ed attività di controllo che abbia come obiettivo la riduzione del rischio di commissione dei Reati mediante la individuazione dei Processi Sensibili.
I principi contenuti nel presente Modello sono volti, da un lato, a determinare una piena consapevolezza del potenziale autore del Reato di commettere un illecito (la cui commissione è fortemente condannata da SAN MARCO perché contraria alle norme di deontologia cui essa si ispira e ai suoi interessi, anche quando apparentemente la Società potrebbe trarne un vantaggio), dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire alla società stessa di reagire tempestivamente nel prevenire od impedire la commissione del Reato stesso.
Tra le finalità del Modello vi è, quindi, quella di sviluppare nei Dipendenti, nei membri degli Organi Societari, nei Consulenti e Partner che operano nell'ambito dei Processi Sensibili, la consapevolezza di poter determinare – in caso di comportamenti non conformi alle prescrizioni del Modello e alle altre norme e procedure aziendali (oltre che alla legge) – illeciti passibili di conseguenze penalmente rilevanti.

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

La logica seguita e le modalità della mappatura dei rischi: la metodologia *top down*

Le finalità di un sistema orientato all'elaborazione del modello organizzativo secondo le specifiche ed i requisiti posti dal D.Lgs 231/01, rappresentano un aspetto di novità rispetto alle esperienze abitualmente vissute nell'ambito degli audit aziendali. Per la prima volta infatti l'azienda si trova di fronte alla necessità di prevenire la commissione di reati; non di reati qualunque, ma di reati commessi nel proprio interesse o a proprio vantaggio.
E' di tutta evidenza la difficoltà di ordine logico e strutturale che si può incontrare, già nell'identificare le aree di attività nel cui ambito tali fatti possano tradursi in concrete fattispecie criminose, prima ancora che nel dettare regole di comportamento finalizzate alla prevenzione di fatti in qualche modo vantaggiosi per l'ente.
Il superamento di questa difficoltà richiede uno sforzo ulteriore e diverso rispetto a quello abitualmente affrontato dall'azienda nelle consuete operazioni di audit, finalizzate alla gestione del sistema qualità. E' evidente infatti che per quest'ultima finalità la mappatura dei processi aziendali scaturisce da una logica che prende in considerazione tali processi come emergono dalle dichiarazioni dei responsabili delle funzioni interessate nel corso del processo di audit.
L'Istituto di studi sulla responsabilità amministrativa degli enti (Istituto ISR), ha valutato che tale modo di procedere non garantisce le finalità di prevenzione dei reati presupposto, che dovrebbero invece caratterizzare l'analisi dei rischi nell'ambito di un sistema 231. Si è stabilito quindi di mettere a frutto l'esperienza dei penalisti d'impresa, unita a quella degli esperti organizzativi, nel singolare connubio che è il punto di forza della consulenza dell'Istituto ISR: ciò ha consentito di identificare una serie di attività di funzione che per la loro stessa natura, presentano un livello di rischiosità intrinseco, tale da necessitare un approfondimento, benché tali attività di funzione non fossero state mappate nel corso degli audit sulla qualità.
Il percorso di questo approfondimento rappresenta la fase di risk analysis del sistema 231; gli esiti del processo di audit possono portare ad escludere che l'attività esaminata costituisca un processo sensibile relativamente ai rischi di reato: in tal caso il valore della risk analysis sarà quello di avere comunque preso

in considerazione tale attività e la posizione attuale dell'azienda nei suoi confronti; in caso contrario l'identificazione di un'attività come processo sensibile, scaturisce dall'audit in relazione ad essa, ed evidenzia le azioni correttive che possono ricondurre il processo sensibile ad un livello di rischio accettabile o nullo. Si tratta della metodologia che l'Istituto ISR definisce “top down”, in contrapposizione a quella tipica dei sistemi di gestione della qualità, che potremmo definire “bottom up”.

La costruzione del Modello e la sua struttura

SAN MARCO ha dato vita ad un progetto interno finalizzato a predisporre il Modello di cui agli artt. 6 e 7 del D.Lgs. 231/01 e dell’art. 30 del D.lgs. 81/08.
Si descrivono qui di seguito la metodologia e le fasi in cui si è articolato il lavoro di individuazione delle aree a rischio, sulle cui basi si è poi dato luogo alla predisposizione del presente Modello.

La prevenzione dei reati e l’integrazione dei sistemi

La necessità più importante, a seguito dell’introduzione delle nuove figure di reato appare agli operatori ed alle imprese e cooperative quella di realizzare una efficace integrazione fra i sistemi di gestione che risultano applicati all’organizzazione aziendale: si pensi ad un’organizzazione che con impegno e sforzo abbia conseguito importanti certificazioni come la
UNI – EN ISO 9001
OHSAS 18001
ISO 22001
ISO 14001
SA 8000
E molte altre, e le mantenga attraverso impegnativi percorsi di audit e verifica.
Tuttavia la complessità di un tale sistema richiede in modo ormai indispensabile l’effettiva integrazione dei sistemi di gestione nel suo complesso e più in

particolare delle normative e dei meccanismi messi in atto per la loro corretta osservanza.
La mancanza di integrazione si traduce in:

- sovrapposizione di normative
- sovrapposizione di politiche
- sovrapposizione di procedure
- proliferazione di documenti cartacei
- replicazione di organismi e autorità di controllo
- potenziale conflitto fra questi.

Tali problemi, oltre a costituire un dispendio economico considerevole, rallentano le procedure, ostacolano la loro osservanza, e in definitiva, minano la loro efficacia ed efficienza del sistema.
Di più: questa mancanza di efficacia ed efficienza mette in crisi l'idoneità del sistema organizzativo nella prevenzione dei reati presupposto.
Qualora infatti venisse commesso uno di tali reati il Giudice, nell'indagine sull'idoneità del modello organizzativo, non potrebbe che riscontrare le notevoli difficoltà nell'attuazione effettiva delle regole contenute nel modello stesso e nelle procedure che vi danno attuazione nell'ottica anche delle certificazioni sopra richiamate.
E' giurisprudenza affermata infatti quella secondo cui le certificazioni in se' non sono sufficienti a garantire la presenza di un efficace modello organizzativo per la prevenzione dei reati.

I moderni strumenti per la gestione della responsabilità: il sistema CLOUDGOVERNANCE 2.0

L'Istituto ISR ha elaborato nel corso della propria esperienza di realizzazione dei modelli organizzativi, una tecnologia efficace per la integrazione dei sistemi nell'ottica di un'idonea prevenzione dei reati presupposto. Tale tecnologia, basata su un servizio on-line denominato Cloudgovernance, consente di mantenere

sotto controllo costante anche in remoto i seguenti aspetti dei sistemi di gestione e del modello organizzativo 231:

- attività sensibili
- manuali dei sistemi di certificazione
- procedure operative
- documenti e comunicazioni
- personale e figure operative coinvolte e relative responsabilità
- scadenze
- misurazioni e statistiche della pericolosità

Oltre a ciò il sistema Cloudgovernance consente di gestire in modo diretto e avvalendosi dello strumento informatico alcuni delicatissimi processi relativi alla gestione di:

- Dispositivi di Protezione Individuale
- Attrezzature
- Infortuni sul lavoro
- Gare d'appalto

Tutti estremamente rilevanti per la realizzazione dei reati presupposto.
Questi aspetti di gestione dei processi sono perfettamente integrati nel sistema Cloudgovernance e intrecciano in dati ed i documenti relativi, con tutti gli strumenti dedicati all'analisi dinamica delle attività sensibili e delle relative pericolosità, contribuendo in modo determinante alla prevenzione dei reati.
Solo in tal modo il Modello Organizzativo 231 diventa una realtà dinamica e costantemente aggiornata, e si prepara ad esercitare la propria efficacia esimente della responsabilità penale della persona giuridica.
L'accessibilità dei dati e documenti in remoto consente anche una più efficace azione dell'Organismo di Vigilanza, rendendo più immediato e completo l'intervento di verifica e, conseguentemente, più credibile la sua azione di fronte ad eventuali indagini dell'Autorità Giudiziaria a seguito di commissione di reati.
Il sistema risiede su una piattaforma web garantita in modo assoluto da ogni accesso indesiderato attraverso le più moderne tecnologie di *cloud computing*, di *firewalling* e di protezione dei dati in transito. L'accesso utente avviene unicamente attraverso la fornitura di *username* e *password* dedicati all'utente e differenziati in base alle proprietà del singolo utente ed alle autorizzazioni di lettura e modifica dei dati.

Un modello organizzativo realizzato con la nuova tecnologia Cloudgovernance diventa quindi un vero Sistema Integrato di Gestione della Responsabilità.

La realizzazione del Modello Organizzativo Integrato presso SAN MARCO

L'impegno necessario alla realizzazione del Modello Organizzativo Integrato presso SAN MARCO è stato relativamente favorito dal buon livello di sviluppo dei sistemi di gestione, che si presentavano completi ed uniformi nelle metodologie applicative.
Ciò ha consentito di approcciare la implementazione del sistema Cloudgovernance attraverso un'attività di caricamento dei dati e dei documenti, nell'ambito delle necessarie sessioni di audit per la mappatura delle attività sensibili per i reati introdotti fra le fattispecie di reato presupposto ex artt. 24 e sgg. D.lgs. 231/2001.
L'Istituto di Studi sulla Responsabilità amministrativa degli Enti ha messo a disposizione le competenze e l'attività dei propri consulenti per effettuare concretamente la migrazione dei dati e documenti nel sistema Cloudgovernance, e predisporre il sistema alla misurazione ed analisi dei dati così introdotti, nonché all'integrazione dei sistemi specifici dedicati alla gestione dei DPI, Infortuni, Attrezzature e Gare d'appalto, con il relativo caricamento dei dati e documenti.
L'incarico dei consulenti dell'Istituto di Studi sulla Responsabilità amministrativa degli Enti è consistito anche nell'assistere le funzioni aziendali coinvolte, nonché il Presidente ed il Consiglio d'Amministrazione, nella prima fase di attuazione del sistema Cloudgovernance, al fine di affiancare la migrazione dell'operatività su tutti i fronti, documentale e gestionale, e consentire di raccogliere le eventuali osservazioni e proposte per adattamenti e personalizzazioni del sistema.

GESTIONE DEI RISCHI AZIENDALI SECONDO IL D.Lgs n 231/01

La gestione dei rischi svolta in base alla logica che abbiamo descritta, impone agli auditors di dotarsi di un'adeguata strumentazione tecnologica che risponda ai seguenti requisiti:

–flessibilità;
–stabilità;
–potenzialità di calcolo;
–compatibilità;
–efficacia grafica e di rappresentazione.

La scelta dell'Istituto di Studi sulla Responsabilità Amministrativa degli Enti si è orientata verso un applicativo su base *web*, consistente in una mappatura delle attività sensibili, ed una adeguata strumentazione informatica che consenta di gestire in modo efficace ed efficiente le responsabilità di impresa, rendere costantemente reperibili i documenti relativi, tenere sotto controllo adempimenti e scadenze in tema di sicurezza del lavoro (formazione, DPI, attrezzature), gestire in modo efficiente la contrattazione con la Pubblica Amministrazione.

Il cuore del Modello Organizzativo Integrato è rappresentato dal sistema denominato Cloudgovernance, che è stato sviluppato sulla base della pluriennale esperienza dei consulenti di dell'Istituto di Studi sulla Responsabilità Amministrativa degli Enti, ed arricchito con alcune soluzioni proposte dai ricercatori del Dipartimento di Economia Aziendale dell'Università degli Studi di Verona, nell'ambito di un programma di ricerca comune che ha condotto fra le altre cose, alla realizzazione di alcune tesi di laurea in materia di modelli organizzativi 231.

Il sistema è stato progettato per rispondere ai seguenti requisiti:

–rappresentare le attività di funzione potenzialmente sensibili;

–consentire l'identificazione dei responsabili di processo;

–guidare nella rappresentazione della situazione "as is";

–svolgere una valutazione oggettiva delle performances

–guidare nell'identificazione ed attuazione delle azioni correttive;

–consentire un accesso immediato alle procedure coinvolte ed a tutti i documenti aziendali;

–tenere sotto controllo le scadenze di azioni correttive, procedure, DPI, attrezzature, gare d'appalto;

–gestire direttamente i processi più rischiosi (come ad esempio la partecipazione a gare d'appalto).
Il risultato raggiunto costituisce una esclusiva di Istituto di studi sulla responsabilità amministrativa degli enti, e si differenzia radicalmente per la sua efficacia da ogni altra esperienza in questo ambito. Il sistema Cloudgovernance in tal modo è il cuore del sistema 231, punto nevralgico intorno a cui ruotano tutte le altre applicazioni, che fanno riferimento ad essa ed alle sue costanti evoluzioni.
A questo punto si inseriscono le attività volte all'implementazione del sistema di gestione della responsabilità presso SAN MARCO ; tali attività si possono così schematizzare:

MODULO A: ANALISI DEI RISCHI AZIENDALI	MODULO A.1: ANALISI DEI RISCHI AZIENDALI: Viene effettuata una prima Analisi dei Rischi Aziendali relativi ai reati presupposto 231, inclusi quelli inerenti la sicurezza dei lavoratori e la corretta gestione ambientale, al fine di individuare le priorità d'intervento. Vengono rivisti e riutilizzati i dati già assunti nella prima analisi del 2009. MODULO A.2: MISURAZIONE DELLE PERFORMANCES: La risk analysis viene effettuata sulla base della esperienza e tecnologia dell'Istituto ISR, con il metodo denominato "Top Down", che parte dall'analisi dei reati-presupposto e delle corrispondenti attività sensibili, per confrontarle con la situazione as-is dell'azienda nel corso del processo di audit. Ne scaturisce una misurazione del livello di pericolosità attuale, attraverso un collaudato schema di algoritmi di calcolo. In base ai risultati di tale analisi verranno quindi stabiliti, di concerto con il cliente, gli indirizzi e le priorità delle azioni correttive. MODULO A.3: INSERIMENTO DELLE ATTIVITA' SENSIBILI IN CLOUDGOVERNANCE I dati relativi alle attività sensibili, quali risultanti dalla risk analysis effettuata come al modulo A.1, vengono inseriti nel

sistema Cloudgovernance con le relative scadenze di azioni di miglioramento ritenute necessarie.

MODULO B: ORGANIGRAMMA: RUOLI, RESPONSABILITÀ, INCARICHI ED EVENTUALI DELEGHE

MODULO B.1: VERIFICA DELL'ORGANIGRAMMA

La verifica dell'organigramma aziendale è svolta in funzione della individuazione degli incarichi e delle eventuali deleghe da attribuire a Dirigenti, Preposti, del personale dell'organizzazione ed eventuali consulenti esterni, relativamente alla prevenzione di tutti i reati presupposto ex D.lgs. 231/2001 nonché alle responsabilità per la sicurezza e l'ambiente.

MODULO B.2: EVENTUALI DELEGATI

Il Datore di Lavoro può, sulla base delle nuove norme, delegare poteri e responsabilità in materia di sicurezza sul lavoro e ambientale a soggetti, anche interni all'azienda, dotati delle necessarie competenze e muniti di autonomia di poteri e di budget adeguato. La designazione del Delegato può implicare esonero di responsabilità penale del Datore di Lavoro ed esonero di responsabilità amministrativa dell'azienda, previo controllo dell'attività del Delegato da parte dell'Organismo di Vigilanza. Il consulente procede, nel caso il Datore di Lavoro intenda delegare le responsabilità, a fornire tutte le informazioni necessarie, sul piano legale ed operativo, sia al Delegante che al Delegato. Il Delegato, a sua volta, può subdelegare specifiche responsabilità ad altri dipendenti. La creazione di un'adeguata rete di Delegati, al di là dell'esonero di responsabilità, se gestita secondo le prescrizione del Modello Organizzativo, migliora senz'altro gli standard di sicurezza sul lavoro e ambientale.

L'opportunità di ricorrere ad un sistema di deleghe dovrebbe essere valutata prima dell'inizio degli interventi formativi per consentire ai futuri delegati di partecipare alle varie attività in funzione delle responsabilità che andranno ad assumere.

In ogni caso le attività di consulenza ed assistenza legale per l'istituzione del sistema di deleghe in materia di sicurezza e ambiente, sono svolte dai legali incaricati.

MODULO B.3: INSERIMENTO DELL'ORGANIGRAMMA IN CLOUDGOVERNANCE 2.0

L'organigramma di SAN MARCO viene inserito nel sistema Cloudgovernance con l'indicazione delle figure di riferimento per l'integrazione delle stesse con tutti gli strumenti operativi e di controllo del sistema stesso. L'organigramma è il fulcro attorno a cui ruotano tutte le potenzialità di integrazione del sistema Cloudgovernance, che in questo caso è effettivamente *user-oriented*, nel senso che è a partire dall'utente (e graficamente proprio dall'organigramma) che vengono prese in considerazione tutte le attività sensibili, le procedure e la pericolosità relativa. Si tratta quindi di una fase molto importante che si è svolta in affiancamento al responsabile delle Risorse Umane.

MODULO B.4: ORGANISMO DI VIGILANZA

Gli amministratori e il Responsabile di Sistema vengono informati sulle competenze previste dal D.Lgs. 231/2001 in relazione all'Organismo di Vigilanza (ODV), incaricato di controllare la corretta attuazione del Modello Organizzativo. Vengono assunte le decisioni relative alla sua individuazione e compiti. È necessario che sia elaborato un Regolamento per il funzionamento dell'Organismo di Vigilanza e che, annualmente, sia predisposto un Piano dei controlli.

MODULO C: REDAZIONE DEL MANUALE

MODULO C.1: REDAZIONE DEL MANUALE:

DEL MODELLO ORGANIZZATIVO 231

Il risultato della risk analysis dà luogo alla formulazione delle modalità operative decisionali, e quindi dà vita al presente manuale del modello organizzativo il quale contiene:

regole di base nel modello organizzativo;

revisione delle procedure in base al processo di auditing svolto nella risk analysis (comprese le revisioni ritenute necessarie sulle procedure aziendali)

stesura di nuove procedure per le aree di processi sensibili non strutturate da quelle esistenti

il modello organizzativo conterrà :

linee di reporting specifiche verso l'organismo di vigilanza (O.d.V.)

facoltà di approfondimento dell'O.d.V. in ogni aspetto dei processi sensibili

linee di reporting dell'O.d.V. verso l'organo dirigente.

Inoltre il modello organizzativo introduce un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

MODULO C.2: INTEGRAZIONE DEI DOCUMENTI E PROCEDURE

I documenti e procedure ritenuti, d'intesa con la Direzione, d'interesse per la gestione della responsabilità, vengono acquisiti ed inseriti nel sistema informatico a cura del personale di Istituto ISR.

Le procedure organizzative vengono catalogate ed inserite nel sistema informatico sulla base dell'area di appartenenza ed indicizzate per le ricerche automatizzate.

MODULO D: PERCORSI FORMATIVI SPECIFICI

Per ognuna delle figure individuate (Amministratori, dirigenti, preposti, lavoratori dipendenti, e collaboratori) vengono sviluppati specifici percorsi formativi al fine di fornire una completa informazione sulle nuove norme, sugli scopi del Modello Organizzativo, sulla corretta gestione delle nuove

responsabilità assegnate. Ciò sia per quanto attiene la sicurezza del lavoro che ai fini della corretta gestione ambientale.
I subappaltatori o collaboratori storici dell'azienda vengono formati sulle nuove norme e sugli scopi del Modello Organizzativo e sui nuovi rapporti contrattuali che verranno perfezionati per garantire la loro adesione al nuovo sistema.

MODULO E: PIANO FINANZIARIO DELLA GESTIONE

La responsabilità amministrativa dell'impresa si previene innanzitutto dimostrando che non si è tratto vantaggio dalla eventuale commissione del reato. E' quindi necessario predisporre un documento dove si indicano i costi sostenuti e da sostenere, anno dopo anno, per prevenire gli illeciti e/o reati presupposto.

MODULO F: GESTIONE CONTRATTUALE

Con il Responsabile del Sistema di Gestione e con l'addetto all'Amministrazione e agli Acquisti verrà effettuato un modulo formativo per l'adeguamento del sistema contrattuale agli adempimenti del Modello Organizzativo (contratto di vendita, di subappalto, di prestazione d'opera, di noleggio e di comodato gratuito).
I Sistemi di Gestione dei diversi aspetti finalizzati alla prevenzione dei reati presupposto, vengono realizzati in una prospettiva che può facilitare il conseguimento delle relative certificazioni, qualora la Direzione Aziendale deliberasse di conseguirle

MODULO G: PRESENTAZIONE DEI DOCUMENTI 231

MODULO H.1: PRESENTAZIONE FORMALE DEI DOCUMENTI:
Esauriti i moduli formativi, vengono presentati dai consulenti i documenti previsti dalle Linee Guida:

Lettere di incarico da attribuire a Dirigenti, RSPP, Preposti, Responsabile di Sistema e Medico Competente;
Eventuali deleghe di funzioni;

MODULO H.2: DELIBERE DI ADOZIONE:
Una volta definite le decisioni di cui al punto precedente, l'Organo Amministrativo aziendale è stato in grado di deliberare l'adozione del Modello Organizzativo, formalizzando l'incarico all'Organismo di Vigilanza e indicando eventualmente i tempi previsti per la certificazione del Sistema di Gestione della Sicurezza del Lavoro e del Sistema di Gestione Ambientale.
Il consulente legale ha assistito l'Organo Amministrativo nella stesura della delibera ed in tutti gli adempimenti collegati.
A partire dalla delibera di adozione, anche se il Sistema di Gestione non è certificato per la parte di sicurezza e per la parte ambientale, i vari incaricati ed i lavoratori fin da subito inizieranno ad adempiere alle regole disciplinari del Modello Organizzativo.

MODULO H: ATTIVAZIONE DEL PORTALE PCC

Una volta definiti i contenuti del sistema integrato Cloudgovernance e caricati nel server web, il portale dedicato a SAN MARCO è stato attivato e sono stati assegnati Username e Password per n. 4 utenti, di cui n. 1 utente con facoltà di caricamento dei dati e n. 3 utenti con facoltà di lettura dei dati.
L'attivazione comporta l'implementazione di una piattaforma di Cloud Server, ovvero un server remoto ad alte prestazioni, con garanzia di stabilità, continuità e riservatezza dei dati. Il contratto ed i termini di garanzia vengono allegati alla documentazione di sistema e consegnati a ciascuna società utente.

Il manuale del modello organizzativo

Il presente Manuale è costituito da una “Parte Generale” e più “Parti Speciali” predisposte per le diverse categorie di reato contemplate nel D.Lgs. 231/01.
La Parte Generale contiene le regole ed i principi generali del Modello.
La Parte Speciale 1, denominata “Reati commessi nei rapporti con la Pubblica Amministrazione”, trova applicazione per le tipologie specifiche di Reati previste ai sensi degli artt. 24 e 25 del D.Lgs. 231/01.
La Parte Speciale 2, denominata “Reati Societari”, si applica per le tipologie specifiche di Reati previste ai sensi dell'art. 25 ter del D.Lgs. 231/01.
La parte speciale 3 si dedica all’analisi e prevenzione del reato di “autoriciclaggio”, e dei reati di criminalità organizzata, ed alle loro interazioni con gli altri reati presupposto.
La parte speciale 4 riguarda i reati previsti nel D.Lgs. 123/07, ed introdotti nel D.Lgs. 231/01, relativi alle lesioni personali colpose ed all'omicidio colposo derivanti da inosservanza delle norme sulla salute e sicurezza nei luoghi di lavoro. La stessa parte speciale si dirige inoltre verso la prevenzione dei delitti contro la personalità individuale.
La parte speciale 5, contempla l'esegesi della normativa inerente l'introduzione dei reati ambientali nelle fattispecie contemplate nel D.Lgs 231/2001.
La parte speciale 6, si dedica all’analisi delle fattispecie di reati informatici ed inerenti alla tutela della privacy, nonché alla loro prevenzione in SAN MARCO

Nell'eventualità in cui si rendesse necessario procedere all'emanazione di ulteriori Parti Speciali, è demandato al Cda di SAN MARCO , il potere di integrare il presente Modello in una fase successiva, mediante apposita delibera.

UTILIZZO DELLA PIATTAFORMA DI GESTIONE DELLA RESPONSABILITA'

La tecnologia dell'Istituto ISR

Le funzionalità di analisi dei rischi, controllo e verifica dei dati, documenti e processi, consultazione dei manuali e procedure, gestione diretta di alcune importanti aree di processo, sono affidate, come si diceva, ad un portale remoto, funzionante in modalità web secondo la tecnologia del cloud computing.

IL SIGNIFICATO DEL CLOUD COMPUTING

In informatica con il termine inglese cloud computing (in italiano nuvola informatica) si indica un insieme di tecnologie che permettono, tipicamente sotto forma di un servizio offerto da un provider al cliente, di memorizzare/archiviare e/o elaborare dati (tramite CPU o software) grazie all'utilizzo di risorse hardware/software distribuite e virtualizzate in Rete.
La correttezza nell'uso del termine è contestata da molti esperti: se queste tecnologie sono viste da alcuni analisti come una maggiore evoluzione tecnologica offerta dalla rete Internet, da altri, come Richard Stallman, sono invece considerate una trappola di marketing.
È noto come, utilizzando varie tipologie di unità di elaborazione (CPU), memorie di massa fisse o mobili come ram, dischi rigidi interni o esterni, Cd/DVD, chiavi USB, eccetera, un computer sia in grado di elaborare, archiviare, recuperare programmi e dati. Nel caso di computer collegati in rete locale (LAN) o geografica (WAN) la possibilità di elaborazione/archiviazione/recupero può essere estesa ad altri computer e dispositivi remoti dislocati sulla rete stessa.
Sfruttando la tecnologia del cloud computing gli utenti collegati ad un cloud provider possono svolgere tutte queste mansioni, anche tramite un semplice internet browser. Possono, ad esempio, utilizzare software remoti non

direttamente installati sul proprio computer e salvare dati su memorie di massa on-line predisposte dal provider stesso (sfruttando sia reti via cavo che senza fili).

FUNZIONE E SVILUPPI

Nonostante il termine sia piuttosto vago e sembri essere utilizzato in diversi contesti con significati differenti tra loro, si possono distinguere tre tipologie fondamentali di servizi cloud computing:[6]

SaaS (Software as a Service) - Consiste nell'utilizzo di programmi in remoto, spesso attraverso un server web. Questo acronimo condivide in parte la filosofia di un termine oggi in disuso, ASP (Application service provider).

DaaS (Data as a Service) - Con questo servizio vengono messi a disposizione via web solamente i dati ai quali gli utenti possono accedere tramite qualsiasi applicazione come se fossero residenti su un disco locale.

HaaS (Hardware as a Service) - Con questo servizio l'utente invia dati ad un computer che vengono elaborati da computer messi a disposizione e restituiti all'utente iniziale.

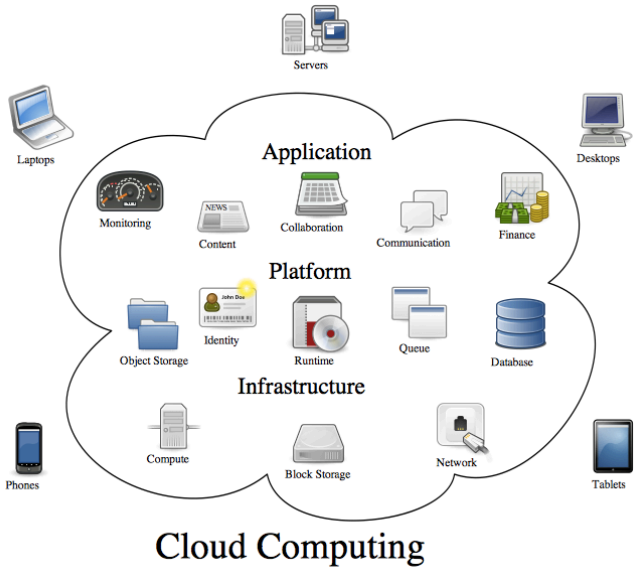
A questi tre principali servizi possono essere integrati altri:

PaaS (Platform as a Service) - Invece che uno o più programmi singoli, viene eseguita in remoto una piattaforma software che può essere costituita da diversi servizi, programmi, librerie, etc. (ad esempio Google's App Engine)

IaaS (Infrastructure as a Service) - Utilizzo di risorse hardware in remoto. Questo tipo di cloud è quasi un sinonimo di **Grid Computing**, ma con una caratteristica imprescindibile: le risorse vengono utilizzate su richiesta o domanda al momento in cui una piattaforma ne ha bisogno, non vengono assegnate a prescindere dal loro utilizzo effettivo.

Il termine cloud computing si differenzia però da grid computing che è invece un paradigma orientato al calcolo distribuito, e in generale, richiede che le applicazioni siano progettate in modo specifico.

Lo schema di massima del cloud computing è rappresentato dalla figura che segue:

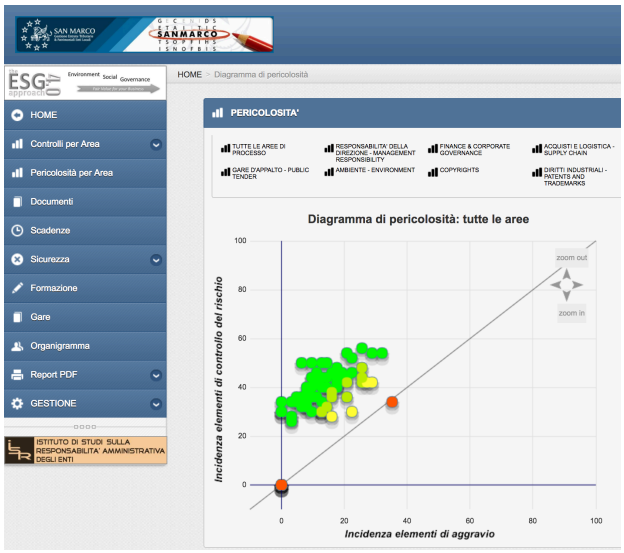


Nel caso di funzionalità di memorizzazione in remoto la creazione di una copia di sicurezza (backup) è automatica e l'operatività si trasferisce tutta online mentre i dati sono memorizzati in server farm generalmente localizzate nei Paesi di origine del service provider.
Il cloud computing rende disponibili all'utilizzatore le risorse come se fossero implementate da sistemi (server o periferiche personali) "standard". L'implementazione effettiva delle risorse non è definita in modo dettagliato; anzi l'idea è proprio che l'implementazione sia un insieme eterogeneo e distribuito – the cloud, in inglese nuvola – di risorse le cui caratteristiche non sono note all'utilizzatore.
Le caratteristiche di utilizzo e le potenzialità di calcolo distribuite consentono di inquadrare quindi il servizio Cloudgovernance offerto da Istituto di Studi sulla Responsabilità Amministrativa degli Enti come una forma particolarmente sofisticata di Cloud Computing, ovvero il Grid Computing.

Utilizzo del sistema

La homepage

Il portale Cloudgovernance dedicato a SAN MARCO si apre con una homepage che contiene il criterio di suddivisione delle tematiche e dei sistemi di gestione, e ne costituisce l'integrazione.
L'integrazione si attua per il fatto che ogni macro area di attività di sistema prevede una valutazione costante della pericolosità risultante dagli audit permanenti sulle attività sensibili.
La homepage si presenta in questo modo:

	Homepage di SAN MARCO
	

Ogni area di processo prevede quindi la possibilità di accedere alle diverse funzionalità specifiche:

- le attività sensibili;
- i documenti

- gli uffici/aree logistiche aziendali interessate dall'area di processo.

Il grafico al centro della schermata home, definito diagramma di Prouty, rappresenta la pericolosità delle singole attività sensibili attraverso il posizionamento delle stesse sul piano cartesiano. Il colore dei punti che rappresentano le attività sensibili indica la gravità della sanzione possibile, calcolata sulla base del complesso sistema di valutazione della pericolosità meglio descritto in seguito.

Nell'area a destra della homepage compare poi lo spazio NEWS, un servizio offerto dall'Istituto ISR volto a mantenere costante l'aggiornamento sulle normative rilevanti in tema di responsabilità amministrativa degli enti.

La barra degli strumenti posizionata a sinistra, sotto il logo aziendale, consente di accedere ai seguenti servizi:

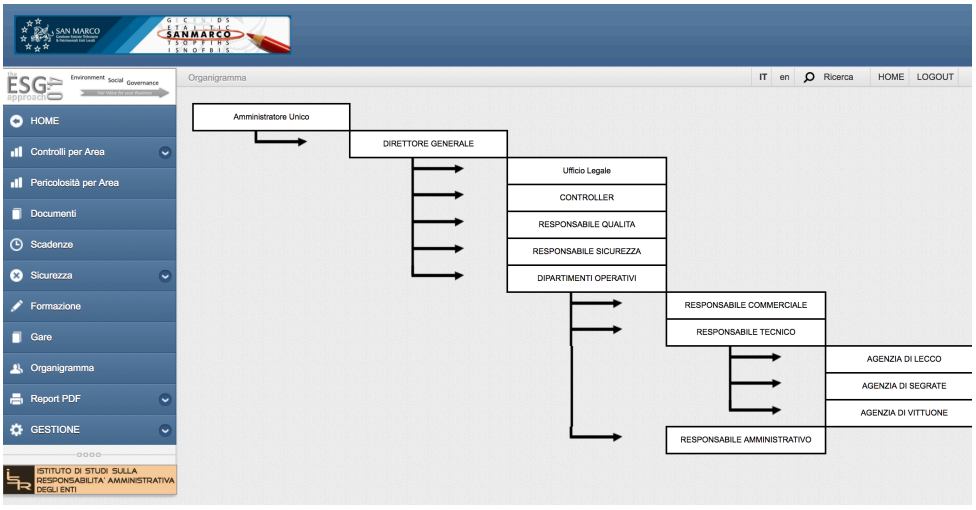
- HOME: in qualsiasi posizione della navigazione è possibile ritornare immediatamente alla homepage;
- SCADENZE: gli utenti a ciò abilitati possono visionare tutte le scadenze inserite nel corso dei processi di audit e relative alle azioni di miglioramento, alle scadenze di attrezzature, DPI e formazione, inserite nell'ambito del processo di audit o nella gestione effettuata con gli specifici applicativi;
- SICUREZZA: apre un menu a tendina che consente di accedere agli applicativi specifici della sicurezza: attrezzature, DPI, registro infortuni.
- GARE: consente l'accesso all'applicativo gestionale delle gare d'appalto, e dei servizi in appalto anche verso imprese private.
- ORGANIGRAMMA: consente l'accesso all'organigramma interattivo;
- GESTIONE: consente agli utenti abilitati l'accesso all'inserimento di dati e documenti.

I seguenti comandi sono posizionati nell'area in alto a destra della homepage:

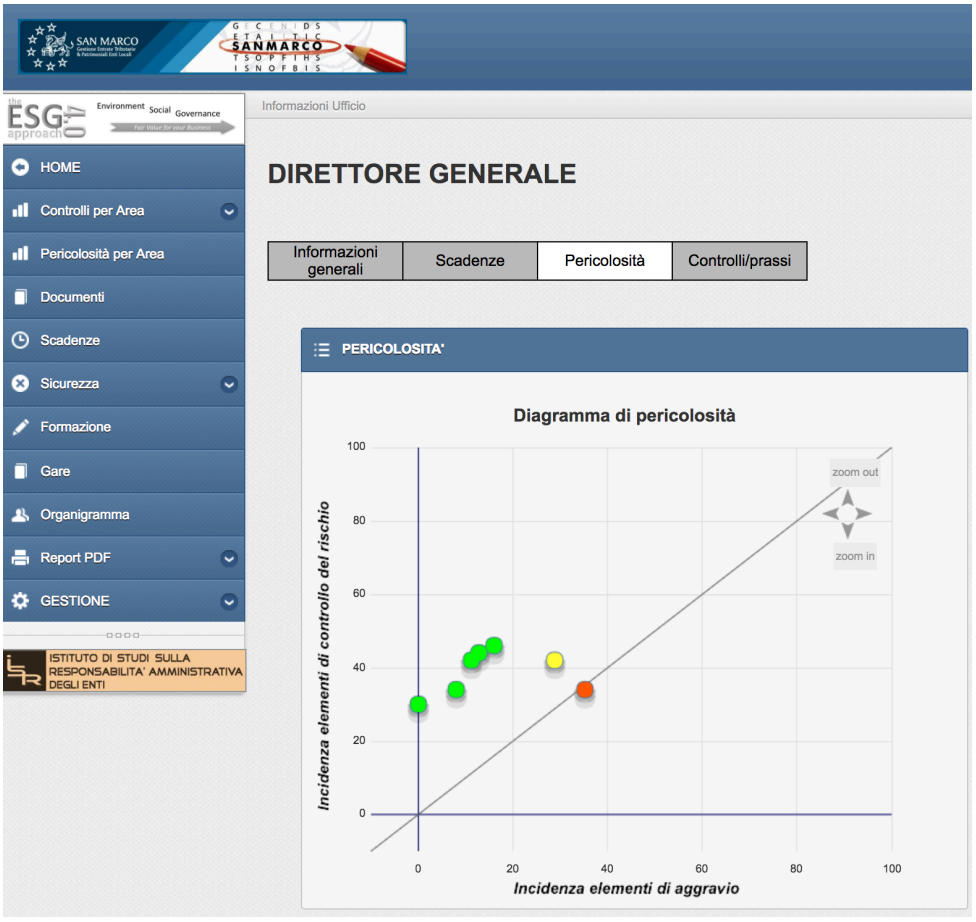
- RICERCA: apre il motore di ricerca nell'intero sistema, per parola o parte di parola.
- LOGOUT: è il comando per disconnettere l'utente.

L'organigramma

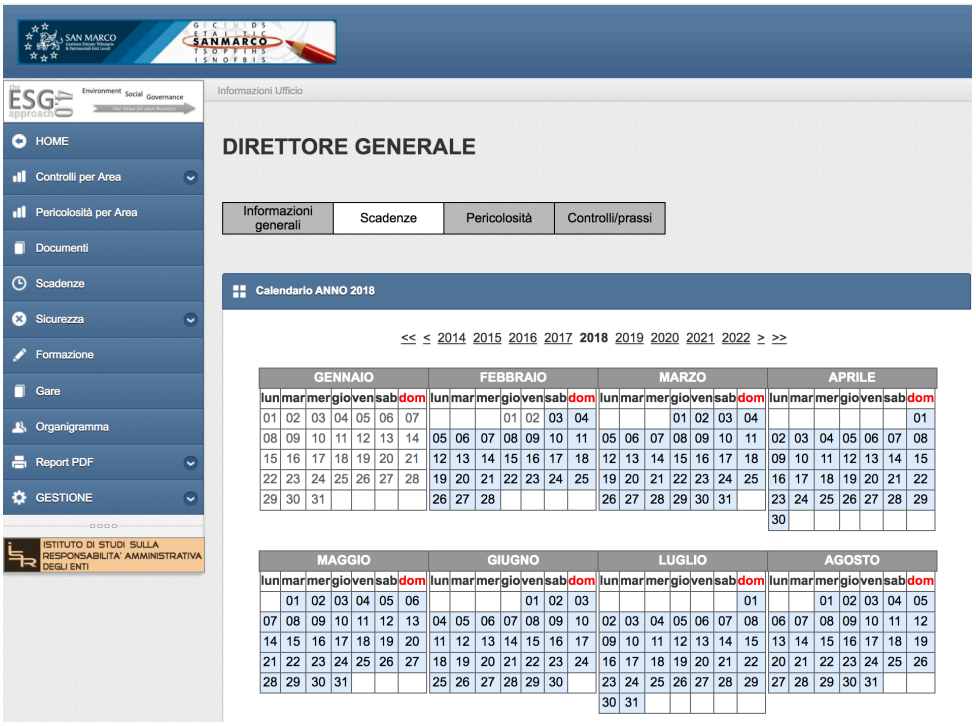
L'organigramma è interattivo ed integrato, nel senso che le funzioni indicate in modo grafico sono attive e conducono alla relativa caratterizzazione in termini di informazioni e contatti, scadenze, pericolosità delle attività, corsi di formazione, controlli svolti sulle attività sensibili.
La grafica dell'organigramma si presenta in questo modo:

	Organigramma SAN MARCO :
	

Cliccando sulle figure dell'organigramma si accede alle diverse attività e pericolosità caratteristica della singola area di processo:

	Organigramma SAN MARCO : pericolosità per singolo ufficio
	

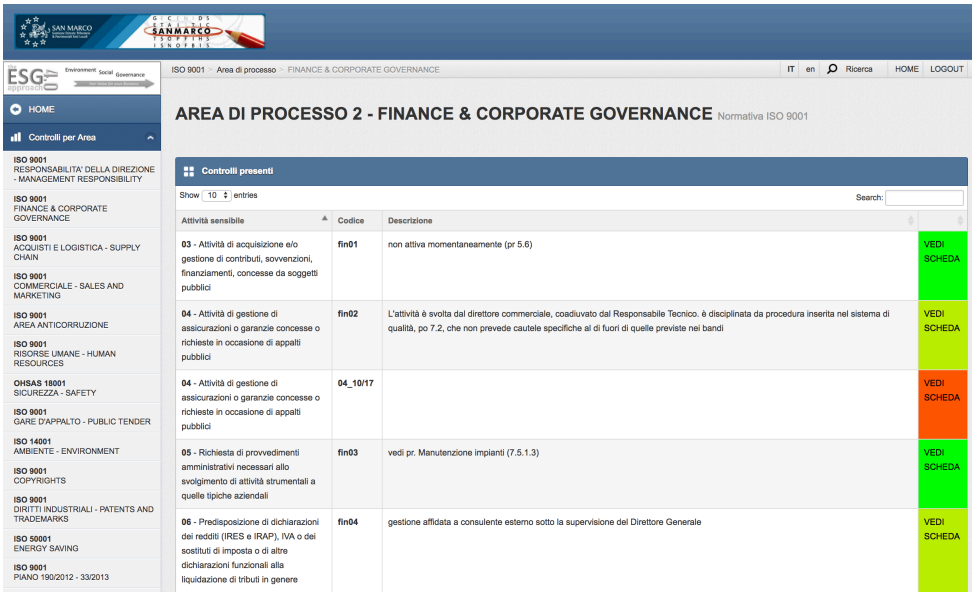
Le scadenze della singola figura di organigramma sono attivabili nel pannello comandi relativo, dove sono presenti unicamente le voci attive per quella figura; per intenderci, se quella figura non è responsabile di alcuna attività sensibile, non avrà alcuna voce di pericolosità e controlli/prassi.
Se in relazione alle attività sensibili vengono assegnate dallo stesso responsabile, o dagli auditors o dai superiori delle scadenze, queste compaiono nella casella relativa:

	Organigramma SAN MARCO : scadenze per singolo ufficio
	

La gestione delle attività sensibili

LE AREE DI PROCESSO

Le attività sensibili sono quelle attività che sono state individuate come astrattamente rischiose per la commissione dei reati presupposto, sulla base dell'esperienza accumulata negli anni dal gruppo di lavoro dell'Istituto ISR, secondo la descritta metodologia TOP DOWN.
Le attività sensibili sono state suddivise in aree di processo, che vengono richiamate direttamente dalla homepage. L'area della Gestione Direzionale viene ulteriormente suddivisa in aree specifiche, che sono rappresentate come segue:

	Attività sensibili SAN MARCO : le aree di processo appaiono nella colonna a sinistra
	

LA LISTA DELLE ATTIVITÀ SENSIBILI

Le aree specifiche aprono la lista delle attività sensibili, che contiene anche la elencazione dei relativi controlli di gestione, che possono anche essere molteplici, a seconda che riguardino specifici uffici o stabilimenti; ciascuna attività sensibile potrà quindi essere controllata da diversi uffici/ responsabili, oppure

venire considerata in modo diverso a seconda della posizione logistica, ad esempio in diversi uffici o stabilimenti periferici.
In tal modo si può avere un controllo sintetico sia dal punto di vista dell'attività sensibile, e vedere le diverse pericolosità che presenta rispetto ai controlli che riceve nei vari uffici/stabilimenti in cui viene applicata, sia una panoramica delle attività sensibili per ufficio/stabilimento, partendo invece dall'organigramma come visto nel paragrafo precedente.

SCHEDA DI CONTROLLO DEL RISCHIO

L'individuazione della pericolosità di ciascuna attività sensibile passa attraverso l'effettuazione di un attento processo di audit, che consente all'esperto di prevenzione dei reati 231 di focalizzare quali siano le buone prassi attualmente in uso, e descriverle sinteticamente nella casella apposita della scheda di controllo di gestione.
La valutazione della pericolosità scaturisce dalla valutazione di una serie di parametri che aggravano la pericolosità e di un'altra serie di parametri che la riducono.
In seguito verranno indicate le non conformità e le conseguenti azioni di miglioramento, nonché la data attesa per la risoluzione delle non conformità.
Tutto il processo deve essere costantemente documentato, ed i documenti devono essere inseriti nella apposita casella, quella relativa alla situazione di partenza e quella relativa alla risoluzione delle non conformità.

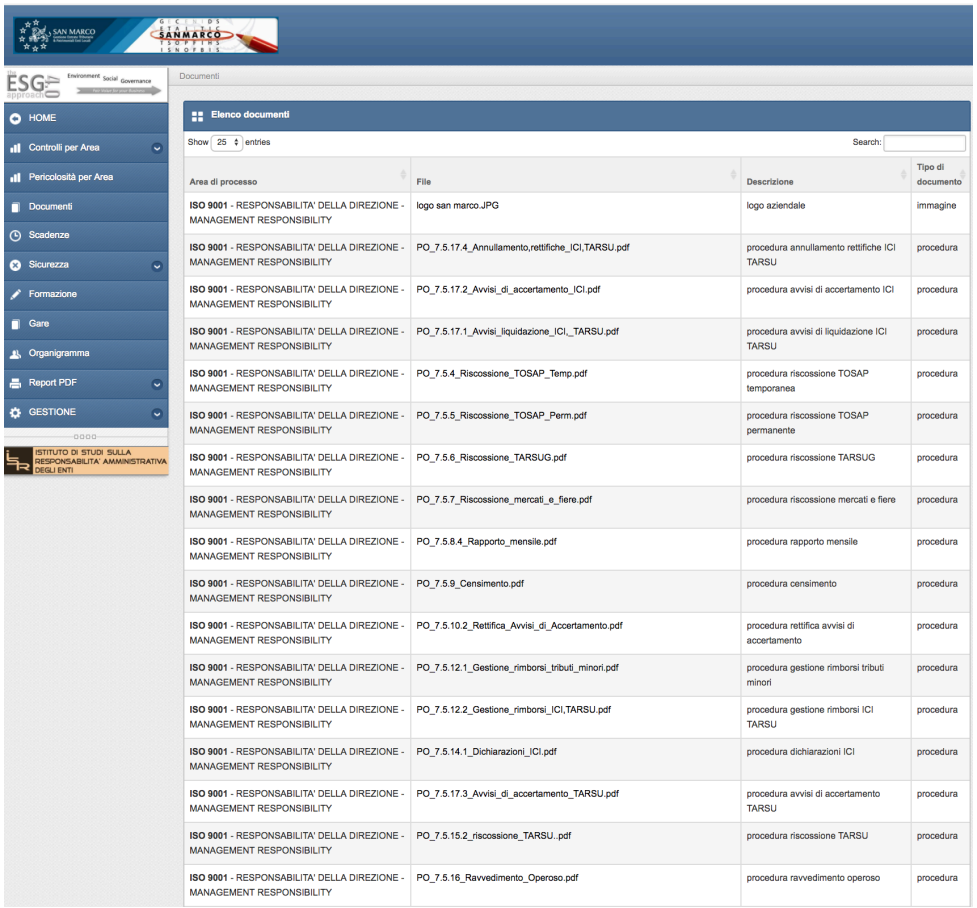
	Attività sensibili SAN MARCO : scheda di controllo

In seguito alla risoluzione della non conformità, ed alla lettura della documentazione inserita nell'apposita casella, l'auditor o il superiore chiudono effettivamente la non conformità, archiviando la scheda di controllo con l'apposito comando.

LA GESTIONE DEI DOCUMENTI

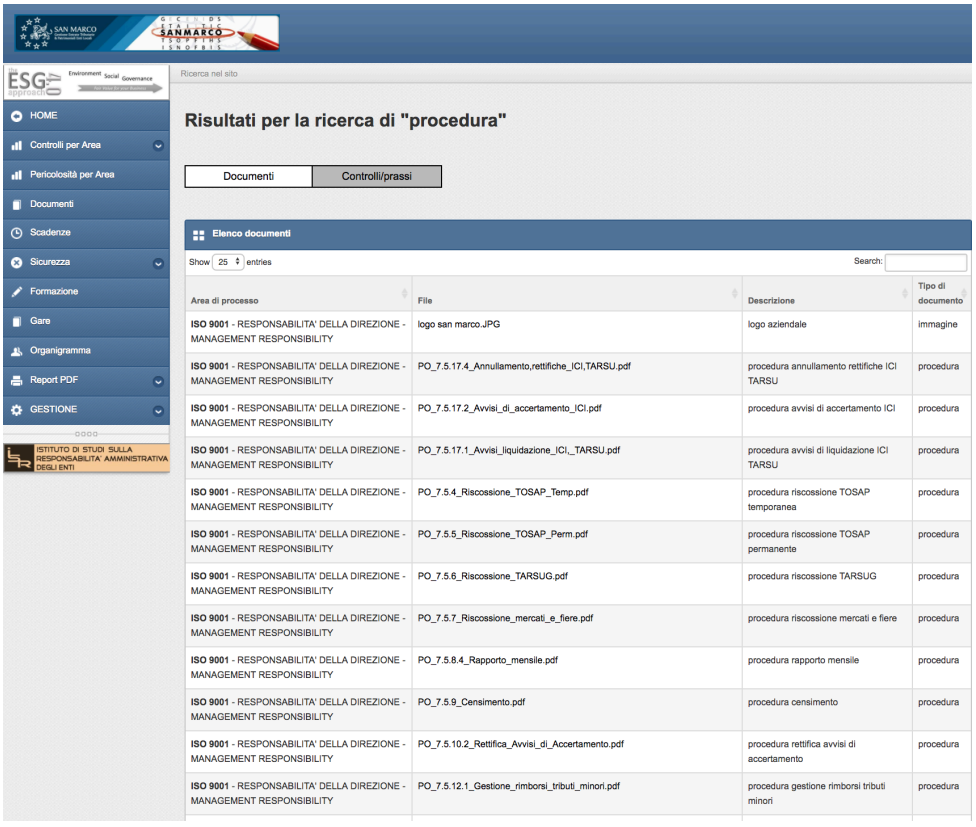
Altrettanto importante la gestione dei documenti, che avviene come da raffigurazione seguente:

Gestione documenti SAN MARCO



La ricerca nel sistema integrato

Il sistema integrato è dotato di un motore di ricerca che consente di trovare, per parola o parte di parola, tutte le ricorrenze, nei documenti, nelle attività, nei controlli, negli applicativi specifici, in modo estremamente semplice e veloce.

	Risultati della ricerca per parola “procedura”
Trova in controlli	

Parte Speciale 1:

Prevenzione dei Reati di corruzione nei rapporti con la Pubblica Amministrazione e con soggetti privati in base alla normativa italiana

Le fattispecie dei reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/01).

La presente Parte Speciale si riferisce ai reati realizzabili nell'ambito dei rapporti tra la Società e la P.A. Si descrivono qui di seguito brevemente le singole fattispecie richiamate nel D.Lgs. 231/01 agli artt. 24 e 25, cui seguono degli esempi astratti di comportamenti vietati da tali norme.

Corruzione fra privati (art. 2635 c.c.)
Tale ipotesi di reato è stata introdotta quale presupposto della responsabilità penale delle persone giuridiche con la l. 190/2012, che ha sancito la punibilità dell'ente per i comportamenti di corruzione posti in essere nell'interesse della Società, verso soggetti che rivestano posizioni decisionali all'interno di un'altra società, per indurlo a compiere atti in contrasto con gli interesse della Società a cui fa riferimento.

Malversazione a danno dello Stato o dell'Unione Europea (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 o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta).
Esempio: uno o più Dipendenti cui sia stata affidata la gestione dei fondi utilizzano gli stessi per scopi diversi da quelli per i quali sono stati erogati (ad es. dei fondi conferiti per scopi formativi o sociali, vengono utilizzati, in parte, per coprire spese di rappresentanza etc.).

Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (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, senza averne diritto, contributi, finanziamenti,

mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dalla Comunità europea.
In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.
Infine, va evidenziato che tale ipotesi di reato, a differenza della fattispecie precedente, si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.
Esempio: un Dipendente della società, allo scopo di ottenere una erogazione da parte delle Comunità Europee, presenta alla competente autorità dei documenti falsamente attestanti l'esistenza in capo alla Società di un requisito indispensabile per l'ottenimento del contributo.

Concussione (art. 317 c.p.)
Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli. Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal D.Lgs. 231/01.

Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318-319-320 c.p.)
Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale italiano o estero riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del suo ufficio (determinando un vantaggio in favore dell'offerente).
L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).
Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.
Esempio: un Dipendente della società offre una somma di danaro ad un funzionario di un ufficio pubblico allo scopo di ottenere il rapido rilascio di un provvedimento amministrativo necessario per l'esercizio dell'attività della società.

Istigazione alla corruzione (art. 322 c.p.)
Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale rifiuti l'offerta illecitamente avanzatagli.

Corruzione in atti giudiziari (art. 319-ter)
Tale ipotesi di reato si configura nel caso in cui la società sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario).
Esempio: un Dipendente offre un'ingente somma di danaro al Pubblico Ministero che conduce indagini penali in merito ad attività svolte dalla società per occultare fatti illeciti ed ottenere l'archiviazione del procedimento.

Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2, n. 1, c.p.)
Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea).
Esempio: un Dipendente, allo scopo di ottenere una licenza od una autorizzazione amministrativa, induce in errore i pubblici ufficiali incaricati facendo apparire agli stessi una falsa rappresentazione della realtà attraverso la produzione di documenti falsi.

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 sia posta in essere per conseguire indebitamente erogazioni pubbliche.
Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.
Esempio: un Dipendente, allo scopo di ottenere delle erogazioni pubbliche induce volontariamente in inganno i pubblici funzionari dell'ufficio competente a decidere della domanda attraverso il concorso di soggetti terzi, i quali, attestino l'esistenza di situazioni fittizie.

Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico dell'ente pubblico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno a terzi.

Funzione della Parte Speciale 1

La presente Parte Speciale si riferisce a comportamenti che possono essere posti in essere dai Dipendenti e dagli Organi Societari di SAN MARCO nonché dai suoi Consulenti e Partner come già definiti nella Parte Generale.
Obiettivo della presente Parte Speciale è che tutti i destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire il verificarsi dei Reati in essa considerati.
Nello specifico, la presente Parte Speciale ha lo scopo di:
• indicare i principi procedurali che i Dipendenti, gli Organi Societari, i Consulenti e Partner di SAN MARCO sono chiamati ad osservare ai fini della corretta applicazione del Modello;
• fornire all'O.d.V. e ai responsabili delle altre funzioni aziendali che cooperano con esso, i principi cui devono ispirarsi gli strumenti esecutivi necessari per esercitare le attività di controllo, monitoraggio e verifica.

a) Criteri per la definizione di Pubblica Amministrazione e di soggetti incaricati di un pubblico servizio: elenco esemplificativo

Obiettivo del presente capitolo è quello di indicare dei criteri generali e fornire un elenco esemplificativo di quei soggetti qualificati come “soggetti attivi” nei reati rilevanti ai fini del D.Lgs. 231/01, ovvero di quei soggetti la cui qualifica è necessaria ad integrare fattispecie criminose previste nel Decreto Legislativo citato.

Pubblici Ufficiali
Ai sensi dell'art. 357, comma 1, c.p., è considerato pubblico ufficiale “agli effetti della legge penale” colui il quale esercita “una pubblica funzione legislativa, giudiziaria o amministrativa”.

Il secondo comma della norma citata si preoccupa poi di definire la nozione di “pubblica funzione amministrativa”. Non si è compiuta invece un'analoga attività definitoria per precisare la nozione di “funzione legislativa” e “funzione giudiziaria” in quanto la individuazione dei soggetti che rispettivamente le esercitano non ha di solito dato luogo a particolari problemi o difficoltà.
Pertanto, il secondo comma dell'articolo in esame precisa 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.
Il secondo comma dell'art. 357 c.p. elenca alcuni dei principali criteri di massima per differenziare la nozione di “pubblica funzione” da quella di “servizio pubblico”.
I caratteri distintivi della prima figura possono essere sintetizzati come segue:

Pubblico Ufficiale:
colui che esercita una pubblica funzione legislativa, giudiziaria o amministrativa.

Pubblica funzione amministrativa:
viene disciplinata da norme di diritto pubblico e da atti autoritativi ed è caratterizzata dalla formazione e manifestazione della volontà della pubblica amministrazione, o dal suo svolgersi per mezzo di poteri autoritativi o certificativi.

Norme di diritto pubblico:
norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico.

Pubblici Ufficiali stranieri:
1. qualsiasi persona che esercita una funzione legislativa, amministrativa o giudiziaria in un paese straniero;
2. qualsiasi persona che esercita una funzione pubblica per un paese straniero o per un ente pubblico o un'impresa pubblica di tale Paese;
3. qualsiasi funzionario o agente di un' organizzazione internazionale pubblica.

Incaricati di un pubblico servizio

La definizione della categoria di “soggetti incaricati di un pubblico servizio” non è allo stato concorde in dottrina così come in giurisprudenza. Volendo meglio puntualizzare tale categoria di “soggetti incaricati di un pubblico servizio”, è necessario far riferimento alla definizione fornita dal codice penale e alle interpretazioni emerse a seguito dell'applicazione pratica. In particolare, l'art. 358 c.p. recita che “sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio”.

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.

Il “servizio”, affinché possa definirsi “pubblico”, deve essere disciplinato – così come la “pubblica funzione” – da norme di diritto pubblico; tuttavia il servizio si caratterizza per l'assenza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

La legge inoltre precisa che non può mai costituire “servizio pubblico” lo svolgimento di “semplici mansioni di ordine” né la “prestazione di opera meramente materiale”.

La giurisprudenza ha individuato una serie di “indici rivelatori” del carattere pubblicistico dell'ente, per i quali è emblematica la casistica in tema di società per azioni a partecipazione pubblica. In particolare, si fa riferimento ai seguenti indici:

(a) la sottoposizione ad un'attività di controllo e di indirizzo a fini sociali, nonché ad un potere di nomina e revoca degli amministratori da parte dello Stato o di altri enti pubblici;

(b) la presenza di una convenzione e/o concessione con la pubblica amministrazione;

(c) l'apporto finanziario da parte dello Stato;

(d) la presenza dell'interesse pubblico in seno all'attività economica.

Sulla base di quando sopra riportato, l'elemento discriminante per indicare se un soggetto rivesta o meno la qualità di “incaricato di un pubblico servizio” è rappresentato, non dalla natura giuridica assunta o detenuta dall'ente, ma dalle funzioni affidate al soggetto le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

I caratteri peculiari della figura dell'incaricato di pubblico servizio sono sintetizzati di seguito definendo tale soggetto come colui che a qualunque titolo, presta un pubblico servizio ovvero un'attività:
1. disciplinata da norme di diritto pubblico;
2. caratterizzata dalla mancanza da poteri di natura deliberativa, autorizzativi e certificativi (tipici della Pubblica funzione amministrativa);
3. mirata alla cura di interessi pubblici o al soddisfacimento di bisogni di interesse generale.
Non può mai costituire pubblico servizio lo svolgimento di semplici mansioni di ordine né la prestazione di opera meramente materiale .

b) Criteri per la definizione dei manager indicati nell'art. 2635 c.c.

L'art. 2635 c.c. identifica ai commi 1 e 2 i soggetti che possono divenire destinatari di attività corruttiva analoga a quella considerata per i Pubblici Ufficiali ed Incaricati di Pubblico Servizio:

1) *gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori;*
2) *chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma*

Le figure indicate al comma 1 sono identificate in modo diretto e chiaro, e non pongono particolari problemi. Quelle richiamate al comma 2 invece sono oggetto di un rinvio generale, che si presta a ricomprendere la più vasta tipologia di funzioni aziendali e posizionamento gerarchico. La caratteristica necessaria è quella di detenere un potere decisionale in merito ai rapporti commerciali o comunque di interesse economico che coinvolgano le due società, ovvero quella ipoteticamente "corruttrice" e quella potenzialmente vittima del manager corrotto.
A titolo meramente esemplificativo si indicano alcune figure generalmente presente nel management aziendale, che potrebbero corrispondere alla tipologia rappresentata al punto 2):

- *responsabile acquisti e logistica;*
- *responsabile IT;*

- *responsabile commerciale;*
- *responsabile qualità;*
- *responsabile sicurezza e ambiente;*
- *responsabile HR;*
- *responsabile bilancio e fiscalità;*
- *responsabile di produzione.*

I manager indicati potrebbero essere fatti oggetto di proposte corruttive per ottenere vantaggi o favori che rappresentino un concreto interesse per la società "corruttrice" nel senso indicato al punto precedente, qualora ciò si rendesse necessario per superare o forzare le corrette dinamiche commerciali e di concorrenza.

Attività Sensibili nei rapporti con la Pubblica Amministrazione e con i soggetti privati

Le principali attività che SAN MARCO ha individuato al proprio interno come Aree Sensibili nei rapporti con la Pubblica Amministrazione e con i soggetti privati, in relazione ai reati di corruzione e di corruzione fra privati, sono le seguenti:

- *gestione del processo commerciale*
- *gestione del patrimonio mobiliare;*
- *rapporti con le istituzioni e con le autorità di vigilanza;*
- *gestione delle ispezioni da parte della Pubblica Amministrazione;*

Regole generali

Il sistema in linea generale

Tutte le Attività Sensibili devono essere svolte conformandosi alle leggi vigenti, alle procedure ed ai regolamenti aziendali rilevanti nonché alle regole contenute nel presente Modello.
Il sistema di organizzazione della società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione dei ruoli, in particolare, per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.
Gli strumenti organizzativi della società (organigrammi, comunicazioni organizzative, procedure, ecc.) devono essere improntati a principi generali di:
a) conoscibilità all'interno della società;
b) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri;
c) chiara descrizione delle linee di report.
In linea di principio, il sistema di deleghe e procure deve essere caratterizzato da elementi di “sicurezza” ai fini della prevenzione dei Reati (rintracciabilità ed evidenziabilità delle Attività Sensibili) e, nel contempo, consentire comunque la gestione efficiente dell'attività aziendale.
Si intende per “delega” quell'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative. Si intende per “procura” il negozio giuridico unilaterale con cui la società attribuisce ad un soggetto dei poteri di rappresentanza nei confronti dei terzi. Ai titolari di una funzione aziendale che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza vengono conferite delle procure di estensione adeguata e coerente con le funzioni ed i poteri di gestione attribuiti al titolare attraverso la “delega”.
I requisiti essenziali del sistema di deleghe, ai fini di una efficace prevenzione dei Reati sono i seguenti:
a) tutti coloro che intrattengono per conto di SAN MARCO rapporti con la P.A. e con i soggetti privati, devono essere dotati di delega formale in tal senso;

b) le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;
c) ciascuna delega deve definire in modo specifico ed inequivoco i poteri del delegato e il soggetto (organo o individuo) cui il delegato riporta gerarchicamente ed, eventualmente, gli altri soggetti ai quali le deleghe sono congiuntamente o disgiuntamente conferite;
d) i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
e) il delegato deve disporre di poteri di spesa ed amministrativi adeguati alle funzioni conferitegli.
I requisiti essenziali del sistema di attribuzione delle procure, ai fini di una efficace prevenzione dei Reati sono i seguenti:
a) le procure, sia speciali che generali, sono conferite esclusivamente a soggetti dotati di delega interna;
b) le procure descrivono i poteri di gestione conferiti e, ove necessario, sono accompagnate da apposita comunicazione aziendale che fissi l'estensione di poteri di rappresentanza ed i limiti di spesa numerici;
c) la procura può essere conferita a persone fisiche espressamente individuate nella procura stessa, oppure a persone giuridiche, che agiranno a mezzo di propri procuratori investiti, nell'ambito della stessa, di analoghi poteri;
d) una procedura ad hoc deve disciplinare modalità e responsabilità per garantire un aggiornamento tempestivo delle procure, stabilendo i casi in cui le procure devono essere attribuite, modificate e revocate (assunzione o estensione di nuove responsabilità e poteri, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, dimissioni, licenziamento, revoca, ecc.);
e) le procure indicano gli eventuali altri soggetti cui sono conferiti congiuntamente o disgiuntamente, in tutto o in parte, i medesimi poteri di cui alla procura conferita.
L'O.d.V. verifica periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative (tali sono quei documenti interni all'azienda con cui vengono conferite le deleghe), raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie.

Principi generali di comportamento

I seguenti principi di carattere generale si applicano, in via diretta, ai Dipendenti e agli Organi Societari di SAN MARCO e, in forza di apposite clausole contrattuali, ai Consulenti ed ai Partner.
Nei rapporti con i soggetti indicati al precedente punto 1.2), è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, considerati singolarmente o complessivamente, siano idonei ad integrare le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del D.Lgs. 231/01). Sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.
Nell'ambito dei suddetti comportamenti è fatto divieto in particolare di:
a) effettuare elargizioni in denaro;
b) offrire doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo il cui valore non sia esiguo o sia eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale).
In particolare non devono essere offerti, né direttamente né indirettamente, qualsiasi regalo, doni o gratuite prestazioni che possano essere o, comunque, apparire connessi con il rapporto di affari con la società o miranti ad influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la società stessa. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore e sono volti a promuovere iniziative di carattere benefico o culturale o l'immagine della società.
Le spese di cortesia in occasione di ricorrenze o, comunque, attinenti la sfera dell'immagine e della comunicazione, ivi comprese le sponsorizzazioni, sono sempre autorizzate dalla Direzione, che ne vaglia la rispondenza ai caratteri ed ai principi sopra esposti. In ogni caso, qualora sorgano dubbi in merito alla legittimità di una spesa di cortesia è opportuno sempre richiedere l'autorizzazione anche da parte del proprio superiore gerarchico diretto. Quest'ultimo e il Responsabile Acquisti procedono a darne comunicazione informativa all'O.d.V.
In tutti i casi i regali o gli omaggi o le spese di cortesia devono essere documentati in modo adeguato per consentire le verifiche da parte dell'O.d.V.
Le liberalità di carattere benefico o culturale eccedenti i valori sopra descritti devono restare nei limiti permessi dalle relative disposizioni legali e dal Modello Organizzativo e dal Codice Etico; inoltre la funzione interessata predispone

l'istruttoria e la sottopone alla Direzione. Di tali liberalità e/o contributi viene immediatamente informato l'O.d.V.;
c) accordare, direttamente o indirettamente, vantaggi di qualsiasi natura tali (o effettuati con modalità tali da) costituire una violazione dei principi esposti nel Modello Organizzativo o nel Codice Etico;
d) eseguire prestazioni e riconoscere compensi in favore dei Consulenti o dei Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
e) presentare dichiarazioni non veritiere ad organismi pubblici nazionali, comunitari e internazionali al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
f) destinare eventuali somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

Parte Speciale 2: Reati societari

Le fattispecie dei reati societari (art. 25 ter del D.Lgs. 231/01)

La presente Parte Speciale si riferisce ai reati societari. Si descrivono qui di seguito brevemente le singole fattispecie contemplate nell'art. 25 ter del D.Lgs. 231/01, cui seguono degli esempi astratti di comportamenti vietati da tali norme.

False comunicazioni sociali (artt. 2621 e 2622 c.c.)
Questo reato si realizza tramite l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci, ai creditori o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, idonei ad indurre in errore i destinatari della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene con l'intenzione di ingannare i soci, i creditori o il pubblico; ovvero mediante l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge.
Si precisa che:
• la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
• le informazioni false o omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene;
• la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;
• il reato di cui all'articolo 2622 c.c. è punibile a querela, salvo che si tratti di società quotate.
Esempio: il Consiglio di Amministrazione ignora l'indicazione del Responsabile Amministrativo circa l'esigenza di un accantonamento (rettifica) al fondo svalutazione crediti a fronte della situazione di crisi di un cliente, ed iscrive un ammontare di crediti superiore al dovuto; ciò al fine di non far emergere una perdita che comporterebbe l'assunzione di provvedimenti sul capitale sociale (artt. 2446 e 2447 c.c.).

Falso in prospetto (art. 2623 c.c.)
Tale condotta criminosa consiste nell'esporre nei prospetti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, false informazioni idonee ad indurre in errore od occultare dati o notizie con la medesima intenzione.
Si precisa che:
• deve sussistere la consapevolezza della falsità e l'intenzione di ingannare i destinatari del prospetto;
• la condotta deve essere idonea a trarre in inganno i destinatari del prospetto;
• la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto.
Esempio: il Consiglio di Amministrazione omette consapevolmente di rappresentare nel documento informativo destinato alla pubblicazione a seguito

di una sollecitazione all'investimento rivolta al pubblico, elementi idonei a formare un giudizio veritiero sui titoli (es. elevato grado di rischio dell'investimento).

Falsità nelle relazioni o nelle comunicazioni della società di revisione (art. 2624 c.c.)
Il reato consiste in false attestazioni o nell'occultamento di informazioni concernenti la situazione economica, patrimoniale o finanziaria della società, da parte dei responsabili della revisione contabile, al fine di conseguire per sé o per altri un ingiusto profitto.
La sanzione è più grave se la condotta ha cagionato un danno patrimoniale ai destinatari delle comunicazioni.
Sebbene i possibili autori di questo reato sono i responsabili della società di revisione (reato proprio), è possibile che i componenti degli organi di amministrazione e di controllo e i suoi Dipendenti possano essere coinvolti a titolo di concorso. È, infatti, ipotizzabile il concorso eventuale, ai sensi dell'art. 110 c.p., degli amministratori, dei sindaci, o di altri soggetti della società revisionata, che abbiano determinato o istigato la condotta illecita del responsabile della società di revisione.

Impedito controllo (art. 2625 c.c.)
Il reato consiste nell'impedire od ostacolare, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, ovvero alle società di revisione.
Esempio: un funzionario della Società non fornisce ad un membro del Collegio Sindacale i documenti da questo richiesti nell'esercizio delle proprie attività di controllo, quali, ad esempio, i documenti concernenti le azioni legali intraprese dalla società per il recupero di crediti.

Omessa comunicazione di conflitto di interessi (art. 2629-bis c.c.)
L'articolo 2629 bis contempla una fattispecie di reato omissivo. Il comportamento quindi è punito solo se esiste un obbligo giuridico di attivarsi. In questi casi l'obbligo si rinviene direttamente nella legge.
L'obbligo risulta dall'art. 2391 c.c. che disciplina l'ipotesi in cui l'amministratore si trovi in conflitto di interessi con la società, conflitto che sorge quando questi abbia un interesse per conto proprio o di terzi, in una determinata operazione della società. Tuttavia non sempre l'omessa comunicazione del conflitto comporta l'invalidità della delibera del consiglio di amministrazione: questa omissione può diventare penalmente rilevante, anche se non in tutti i tipi di società, ma, in generale, quando tale omissione provenga da un amministratore di una società quotata nei mercati regolamentati o con titoli diffusi tra il pubblico in misura rilevante.

Formazione fittizia del capitale (art. 2632 c.c.)
Tale ipotesi si ha quando: viene formato o aumentato fittiziamente il capitale della società mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; vengono sottoscritte reciprocamente azioni o quote; vengono

sopravvalutati in modo rilevante i conferimenti dei beni in natura, i crediti ovvero il patrimonio della società, nel caso di trasformazione.
Esempio: gli amministratori danno luogo ad un aumento del capitale sociale per mezzo dell'offerta di azioni per un valore inferiore a quello dichiarato.

Indebita restituzione dei conferimenti (art. 2626 c.c.)
La "condotta tipica" prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche simulata, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli.
Esempio: l'Assemblea della Società, su proposta del Consiglio di Amministrazione, delibera la compensazione di un debito del socio nei confronti della Società con il credito da conferimento che quest'ultima vanta nei confronti del socio medesimo, realizzando in pratica una restituzione indebita del conferimento.

Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)
Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.
Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.
Esempio: l'Assemblea della Società, su proposta del Consiglio di Amministrazione, delibera la distribuzione di dividendi che costituiscono, non un utile di esercizio, ma fondi non distribuibili perché destinati dalla legge a riserva legale.

Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
Questo reato si perfeziona con l'acquisto o la sottoscrizione di azioni o quote sociali o della società controllante, che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.
Si fa presente che 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.
Esempio: l'organo amministrativo procede all'acquisto o alla sottoscrizione di azioni della Società o di una società controllante fuori dai casi di cui agli artt. 2357 e 2359-bis c.c., determinando così facendo una lesione del patrimonio sociale.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori.
Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Esempio: gli amministratori danno luogo ad un'operazione straordinaria di fusione con una società in stato di forte sofferenza, senza rispettare la procedura prevista dall'art. 2503 c.c. a garanzia dei creditori.

Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.
Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.
Essendo il reato ipotizzabile in sede di liquidazione della Società non appare rilevante in questa sede fornire la descrizione di un esempio di condotta criminosa.

Illecita influenza sull'assemblea (art. 2636 c.c.)
La “condotta tipica” prevede che si determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto.
Esempio: il Consiglio di Amministrazione della Società, al fine di ottenere una deliberazione favorevole dell'assemblea e il voto determinate anche del socio di maggioranza, predispone e produce nel corso dell'adunanza assembleare documenti alterati, diretti a far apparire migliore la situazione economica e finanziaria di un'azienda che lo stesso consiglio intende acquisire, in modo da ricavarne un indiretto profitto.

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

In tale fattispecie di reato sono soggetti attivi: gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, 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; nonostante il gran numero di soggetti attivi, si tratta di reato proprio.
Nel testo di legge si identifica il fatto tipico distinguendo due comportamenti diversi, sostenuti da due differenti tipi di dolo.
1. nelle comunicazioni che i soggetti attivi devono, in base alla legge, inviare all'autorità di vigilanza:
a) espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza;
b) occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima.
In entrambe queste ipotesi l'elemento soggettivo è il dolo specifico, perché il reo deve agire al fine di ostacolare l'esercizio delle funzioni di vigilanza.
2. i medesimi soggetti attivi:
a) in qualsiasi forma, anche omettendo le comunicazioni dovute alle autorità di vigilanza, consapevolmente ne ostacolano le funzioni.

Come si vede si tratta di reato a forma libera che può realizzarsi anche con un'omissione, mentre il dolo è generico, poiché l'ostacolare consapevolmente le funzioni delle autorità di vigilanza, più che indicare il fine per il quale agisce il soggetto attivo, sembra voler escludere a priori la possibilità di responsabilità per colpa. È inoltre reato di pericolo.
La pena prevista in tutti e due i tipi di condotta è della reclusione da uno a quattro anni, si tratta quindi di delitto. La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

Funzione della Parte Speciale 2

La presente Parte Speciale si riferisce a comportamenti che possono essere posti in essere dai Dipendenti e dagli Organi Sociali di SAN MARCO , nonché dai suoi Consulenti e Partner come già definiti nella Parte Generale.
Obiettivo della presente Parte Speciale è che tutti i destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire il verificarsi dei Reati in essa considerati.
Nello specifico, la presente Parte Speciale ha lo scopo di:
a) indicare le procedure che i Dipendenti, gli Organi Sociali, i Consulenti e Partner della società sono chiamati ad osservare ai fini della corretta applicazione del Modello;
b) fornire all'O.d.V., e ai responsabili delle altre funzioni aziendali che cooperano con esso, i principi cui devono ispirarsi gli strumenti esecutivi necessari per esercitare le attività di controllo, monitoraggio e verifica.

Attività Sensibili nell'ambito dei reati societari
Le principali attività che SAN MARCO come già esposto nella Parte Generale del presente documento, ha individuato al proprio interno come Aree Sensibili nell'ambito dei reati societari sono:

- *Esercizio delle forme di controllo societario e di direzione di gruppo;*
- *attività di formazione del bilancio;*
- *gestione e comunicazione verso l'esterno di notizie e dati relativi alla Società;*
- *operazioni sul capitale sociale.*

Regole generali

Il sistema in linea generale

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello e, in particolare, a quelle indicate ai successivi paragrafi, gli Organi Societari (e i Dipendenti e Consulenti nella misura necessaria alle funzioni dagli stessi svolte) devono in generale conoscere e rispettare:

- *l'organizzazione, nonché le procedure aziendali e il sistema di controllo della gestione che lo compongono;*
- *la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale;*
- *le norme inerenti il sistema amministrativo, contabile, finanziario, di reporting;*

- *il sistema di comunicazione al personale e di formazione dello stesso;*
- *il sistema disciplinare di cui al CCNL;*
- *in generale, la normativa italiana e tedesca applicabile.*

Principi di comportamento

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali della società, presenti (o futuri in caso di trasformazioni societarie), e dei Dipendenti e Consulenti nella misura necessaria alla funzioni dagli stessi svolte, di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 ter del D.Lgs. 231/01); sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.
La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

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

In conseguenza, è fatto divieto di:
a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società;
b) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società.
c) alterare i dati e le informazioni destinati alla predisposizione dei prospetti informativi;
d) illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della società e sull'evoluzione della sua attività.

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

In particolare, è fatto divieto di agire in modo tale da far si che gli Organi Sociali competenti adottino uno dei seguenti comportamenti o atti:
a) restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
b) ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
c) acquistare o sottoscrivere quote della società fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;

d) effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni poste dalla legge a tutela dei creditori, provocando ad essi un danno;
d) procedere a formazione o aumento fittizi del capitale sociale, attribuendo azioni o quote per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale.

- 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.

In conseguenza, è fatto divieto di:
a) porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte dei soci;
b) determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare.

- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate.

In conseguenza, è fatto divieto di:
a) omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle autorità di vigilanza cui è soggetta l'attività aziendale, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette autorità;
b) esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;
c) porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle autorità pubbliche di vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

L'attività di formazione del bilancio e, in particolare, predisposizione delle comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della società (bilancio d'esercizio e bilancio consolidato corredati dalla relazione sulla gestione, relazioni trimestrali e semestrale, ecc.), devono essere redatti in modo tale che sia garantito il rispetto dei seguenti precetti aziendali:
- i dati e le informazioni, fornite da ciascuna funzione ai fini della redazione dei documenti volti a rappresentare la situazione economica, patrimoniale e finanziaria della società, devono:

-rispondere a principi di chiarezza e completezza;
-essere interpretati in conformità ai criteri contabili utilizzati per la elaborazione dei dati;

• le valutazioni delle singole voci di bilancio e delle relazioni infrannuali devono essere eseguite in conformità alle disposizioni di legge;
• i documenti volti a fornire una rappresentazione della situazione economica, patrimoniale e finanziaria della società devono esporre e illustrare tutte le informazioni e i dati, anche di carattere complementare, da ritenersi necessari al fine di dare una rappresentazione veritiera e corretta della situazione della Società;
• la redazione deve essere effettuata a seguito del preventivo esame e approvazione della Direzione, per ciò che concerne i comunicati stampa riguardanti le informazioni a carattere periodico e le operazioni straordinarie (aumenti di capitale, fusioni, ecc).

Inoltre:
• gli Organi Sociali, i Dipendenti e i Consulenti sono tenuti a mantenere riservati i documenti e le informazioni rilevanti acquisite nello svolgimento delle loro funzioni e a rispettare le procedure dettate per la comunicazione all'esterno di tali documenti e informazioni;
• è fatto assoluto divieto a chiunque di rilasciare interviste a organi di stampa o fare dichiarazioni che si riferiscano a fatti rilevanti che non siano già stati resi pubblici a norma di legge.
• tutte le operazioni sul capitale sociale di SAN MARCO , nonché la costituzione di società, l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni devono essere effettuate nel rispetto delle procedure aziendali all'uopo predisposte;
• è fatto divieto di porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque costituiscano ostacolo allo svolgimento dell'attività di controllo o di revisione della gestione sociale della società da parte del collegio sindacale.

Altre regole finalizzate alla prevenzione dei reati societari in genere

Attività soggette a vigilanza

Con riferimento alle attività della società soggette alla vigilanza di pubbliche autorità in base alle specifiche normative applicabili, al fine di prevenire la commissione dei reati di false comunicazioni alle autorità e di ostacolo alle funzioni di vigilanza, le attività soggette a vigilanza devono essere svolte in base a procedure aziendali, contenenti la disciplina delle modalità e l'attribuzione di specifiche responsabilità in relazione:

- alle segnalazioni periodiche alle autorità previste da leggi e regolamenti;
- alla trasmissione a queste ultime dei documenti previsti in leggi e regolamenti (ad es., bilanci e verbali delle riunioni degli Organi Sociali);
- alla trasmissione di dati e documenti specificamente richiesti dalle autorità di vigilanza;
- al comportamento da tenere nel corso degli accertamenti ispettivi.

I principi a cui tali procedure si informano sono i seguenti:

- attuazione di tutti gli interventi di natura organizzativo-contabile necessari ad estrarre i dati e le informazioni per la corretta compilazione delle segnalazioni ed il loro puntuale invio all'autorità di vigilanza, secondo le modalità ed i tempi stabiliti dalla normativa applicabile;
- adeguata formalizzazione delle procedure in oggetto e successiva documentazione dell'esecuzione degli adempimenti in esse previsti, con particolare riferimento all'attività di elaborazione dei dati;
- nel corso dell'attività ispettiva, deve essere prestata da parte delle funzioni e delle articolazioni organizzative ispezionate la massima collaborazione all'espletamento degli accertamenti. In particolare, devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati ritengano necessario acquisire, previo il consenso del responsabile incaricato di interloquire con l'autorità;
- alle ispezioni devono partecipare i soggetti a ciò espressamente delegati ed essere tenuto informato l'O.d.V. Di tutto il procedimento relativo all'ispezione devono essere redatti e conservati gli appositi verbali. Dell'avvio di ispezioni deve essere tempestivamente informato l'O.d.V., con nota scritta da parte del responsabile della funzione coinvolta.

Altre attività

A fianco delle regole e delle procedure esistenti, si dispone l'attuazione dei seguenti presidi integrativi:

- attivazione di un programma di formazione-informazione periodica del personale rilevante sulle regole e sui reati societari;
- trasmissione all'Autorità competente, con congruo anticipo, di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del

Consiglio di Amministrazione o sui quali esso debba esprimere un parere ai sensi di legge;
• formalizzazione e/o aggiornamento di regolamenti interni e procedure aventi ad oggetto l'osservanza della normativa societaria.

Fermo restando il potere discrezionale dell'O.d.V. di attivarsi con specifici controlli, anche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello) e ferme restando le specifiche attribuzioni di cui al precedente paragrafo, l'O.d.V. effettua periodicamente, anche coadiuvato da soggetti terzi, controlli a campione sulle attività sociali potenzialmente a rischio di commissione di reati societari, al fine di verificare che la gestione concreta di tali attività avvenga in maniera conforme alle regole e coerente con i principi dettati dal presente Modello (esistenza e adeguatezza della relativa procura, limiti di spesa, effettuato reporting verso gli organi deputati, ecc.).
In ragione dell'attività di vigilanza attribuita all'O.d.V. nel presente Modello, a tale organismo viene garantito, in generale, libero accesso a tutta la documentazione aziendale che lo stesso ritiene rilevante al fine del monitoraggio dei Processi Sensibili individuati nella presente Parte Speciale (vedi Parte Generale).

Area responsabilità strategica generale
Devono essere rispettati i limiti di budget di spesa previsti dalle deleghe. Eventuali superamenti di tali limiti dovranno essere preventivamente approvati dal C.d.A. su richiesta del delegato motivata e fornita di idonea documentazione. La delibera di spesa per atti eccedenti i limiti delega deve essere trasmessa all'O.d.V.

I REATI FISCALI

A pochi mesi dal Decreto Fiscale, il D.Lgs. 75/2020 (in vigore dal 30 luglio 2020) estende nuovamente il catalogo dei reati presupposto per la responsabilità dell'ente. La novella richiama fattispecie di diritto penale tributario, ma non solo: viene ampliato anche il novero dei reati in danno alla PA e viene prevista la responsabilità degli enti per i reati di contrabbando.

Reati 231 aggiornati 2020: in gazzetta ufficiale del 15 luglio 2020 è stato pubblicato il decreto legislativo 14 luglio 2020 n. 75, che recepisce la "direttiva europea (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale".

LE FATTISPECIE

PANORAMICA

Quella dell'inserimento dei reati tributari nel novero dei reati presupposto per la responsabilità degli enti ex D.Lgs. 231/2001 è, come noto, una vicenda che risale alla c.d. Direttiva PIF (UE 2017/1371), con cui l'Unione europea ha demandato ai legislatori nazionali l'adozione di misure adeguate a contrastare, anche con gli strumenti del diritto penale, le cc.dd. gravi frodi IVA, con ciò dovendo intendersi quelle condotte caratterizzate da fraudolenza e transnazionalità che recano un danno agli interessi finanziari dell'Unione Europea non inferiore a euro 10 mln.

Nel catalogo dei reati presupposto per l'applicazione delle sanzioni cosiddette amministrative da reato è stato inserito il delitto di frode in pubbliche forniture (art. 356 codice penale), si è integrato l'art. 25 con il riferimento all'Unione Europea quale soggetto finanziariamente leso nei casi di peculato, anche mediante profitto dell'errore altrui (articoli 314 e 316 codice penale) e abuso d'ufficio (articolo 323 codice penale).
Per i reati in materia di imposte sui redditi e sul valore aggiunto ai sensi del decreto legislativo 10 marzo 2000 n. 74, da oggi 30 luglio 2020 sono previste sanzioni amministrative severe (da trecento a cinquecento quote) se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro.
L'art. 25-sexiesdecies, di nuova introduzione, inoltre, aggiunge al catalogo dei reati presupposto il contrabbando, punito con sanzioni da duecento a quattrocento quote, a seconda del valore dei diritti di confine evasi (inferiore o superiore centomila euro).
In tutti questi casi (art. 25-sexiesdecies) si applicano le sanzioni interdittive:

- il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

FOCUS SUI REATI FISCALI

Il Decreto Fiscale ha introdotto la responsabilità amministrativa degli enti per i delitti di:

- dichiarazione fraudolenta di cui all'art. 2 , co. 1 (sanzione pecuniaria fino a 500 quote), all'art. 2, co. 2-bis (sanzione pecuniaria fino a 400 quote) e all'art. 3 (sanzione pecuniaria fino a 500 quote) D.Lgs. 74/2000;
- emissione di fatture o altri documenti per operazioni inesistenti di cui all'art. 8, co 1 (sanzione pecuniaria fino a 500 quote) e all'art. 8, co. 2-bis (sanzione pecuniaria fino a 400 quote), D.Lgs. 74/2000;
- occultamento o distruzione di documenti contabili di cui all'art. 10 D.Lgs. 74/2000 (sanzione pecuniaria fino a 400 quote);
- sottrazione fraudolenta al pagamento di imposte di cui all'art. 11 D.Lgs. 74/2000 (sanzione pecuniaria fino a 400 quote).

Il Decreto Fiscale ha inoltre previsto:
- una circostanza aggravante all'art. 25-quinquiesdecies, co. 2, D.Lgs. 231/2001 (con aumento della sanzione pecuniaria fino a un terzo) per il caso in cui l'ente abbia conseguito un profitto di rilevante entità dall'illecito;
- l'applicazione delle sanzioni interdittive richiamate all'art. 25-quinquiesdecies, co. 3, D.Lgs. 231/2001 (che richiama l'art. 9, co. 2, lett. c), d), ed e)), ossia: il divieto di contrattare con la PA (salvo che per ottenere prestazioni di un pubblico servizio); l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi.

LE ALTRE FATTISPECIE INTRODOTTE

Le novità introdotte dal D.Lgs. 75/2020 in materia di responsabilità degli enti non si esauriscono ai reati tributari.
Viene infatti altresì modificato l'art. 24 D.Lgs. 231/2001, così ampliando il catalogo dei reati in danno alla Pubblica Amministrazione (nella cui ampia nozione deve ora ricomprendersi, secondo la novella che ha interessato l'art. 24, anche l'Unione europea):
- Al comma primo viene aggiunto il delitto di frode nelle pubbliche forniture ex art. 356 c.p., cui consegue una sanzione pecuniaria fino a 500 quote;
- È poi aggiunto un comma 2-bis, che prevede l'applicazione della sanzione pecuniaria fino a 500 quote in caso di frode ai danni del Fondo europeo agricolo

di garanzia e del Fondo europeo agricolo per lo sviluppo rurale (art. 2 L. 898/1986).
Anche per le nuove fattispecie ora richiamate dall'art. 24 è prevista l'applicazione della circostanza aggravante prevista dal co. 2 (per il caso in cui l'ente abbia conseguito un profitto di rilevante entità ovvero dall'illecito sia derivato un danno di particolare gravità: in questo caso la sanzione pecuniaria sarà da 200 a 600 quote) e delle sanzioni interdittive previste dal co. 3, che richiama l'art. 9, co. 2, lett. c), d), ed e), ossia: il divieto di contrattare con la PA (salvo che per ottenere prestazioni di un pubblico servizio); l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi.

Sempre all'area dei reati che recano danno alla PA devono essere ricondotte le fattispecie che il D.Lgs. 75/2020 ha affiancato a quelle già previste all'art. 25, co. 1, D.Lgs. 231/2001:
- I reati di peculato di cui all'art. 314 c.p., primo comma (rimanendo dunque escluso il peculato d'uso) e all'art. 316 (ossia la particolare forma di peculato mediante profitto dell'errore altrui);
- Il reato di abuso d'ufficio di cui all'art. 323 c.p.

Alle predette fattispecie è collegata una sanzione pecuniaria per l'ente fino a 200 quote, "quando il fatto offende gli interessi finanziari dell'Unione Europea".

Infine, il D.Lgs. 75/2020 introduce nel D.Lgs. 231/2001 un nuovo art. 25-sexiesdecies rubricato "Contrabbando", che inaugura la responsabilità degli enti per i reati previsti dal D.P.R. 43/1973 in materia doganale, che prevede (in particolare, si veda l'art. 295, norma fra l'altro interessata da alcune modifiche apportate proprio dal D.Lgs. 75/2020) sanzioni anche penali in caso di mancato pagamento dei diritti di confine. Il nuovo art. 25-sexiesdecies prevede per questi casi:
- La sanzione pecuniaria fino a 200 quote;
- Un'aggravante per il caso in cui l'ammontare dei diritti di confine dovuti superi euro 100.000 (sanzione pecuniaria fino a 400 quote);

L'applicazione delle sanzioni interdittive di cui all'art. 9, co. 2, lett. c), d), ed e), ossia: il divieto di contrattare con la PA (salvo che per ottenere prestazioni di un pubblico servizio); l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi.

IL CATALOGO DEI REATI

I reati fiscali erano già stati inseriti a catalogo con la legge 157/2019 di conversione del decreto legge 124/2019 in vigore dal 25 dicembre 2019, ma rimaneva scoperta l'integrazione con le fattispecie lesive degli interessi finanziari dell'UE.

Si riepilogano, pertanto, i contenuti che da oggi formano il catalogo delle fattispecie che danno corso alla responsabilità amministrativa da reato (sezione terza del decreto legislativo 231/2001):
Art. 24. Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture
Art. 24-bis. Delitti informatici e trattamento illecito di dati
Art. 24-ter. Delitti di criminalità organizzata
Art. 25. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio
Art. 25-bis. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento
Art. 25-bis.1. Delitti contro l'industria e il commercio
Art. 25-ter. Reati societari
Art. 25-quater. Delitti con finalità di terrorismo o di eversione dell'ordine democratico
Art. 25-quater.1. Pratiche di mutilazione degli organi genitali femminili
Art. 25-quinquies. Delitti contro la personalità individuale
Art. 25-sexies. Abusi di mercato
Art. 25-septies. Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro
Art. 25-octies. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio
Art. 25-novies. Delitti in materia di violazione del diritto d'autore
Art. 25-decies. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
Art. 25-undecies. Reati ambientali
Art. 25-duodecies. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare
Art. 25-terdecies. Razzismo e xenofobia
Art. 25-quaterdecies. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati
Art. 25-quinquiesdecies. Reati tributari
Art. 25-sexiesdecies. Contrabbando

ALCUNE CONSIDERAZIONI

L’ampliamento dell’elenco dei reati che danno luogo alla responsabilità amministrativa di cui al decreto legislativo 231/01 impone a chi si è dotato di modello di effettuare un efficace aggiornamento della risk analysis per verificare se, alla luce della normativa aggiornata, si ricada in nuove aree di rischio.
Potrebbe infatti risultare necessario l’adeguamento del modello, per mantenerlo idoneo ed efficace ed essere conforme ai dettami dell’ordinamento, ma

soprattutto utile all'impresa per prevenire la commissione di reati ed evitare sanzioni pesanti in caso, comunque, gli stessi si verifichino eludendo il modello organizzativo.
L'Organismo di Vigilanza ha un ruolo fondamentale nella segnalazione delle necessità di aggiornamento, ma sarà comunque l'Ente, chiamato ad operare in tal senso, proprio per evitare che l'adozione del modello, possa essere vanificata da un mancato aggiornamento proprio in un'area a rischio.

PARTE SPECIALE 3

IL REATO DI AUTORICICLAGGIO ED I REATI DI CRIMINALITA' ORGANIZZATA

Generalità sul reato di Autoriciclaggio

Il reato (nuovo art. 648-ter.1, c.p.) punisce colui che impiega, sostituisce, trasferisce in attività economiche, finanziarie, imprenditoriali o speculative il denaro, i beni o le altre utilità derivanti dal delitto non colposo (di seguito, anche "reato-base") che lo stesso ha commesso o concorso a commettere. Ciò a condizione che la condotta sia idonea a ostacolare concretamente l'identificazione della provenienza illecita della provvista.
Fermo restando che si prevede la non punibilità delle condotte di mero utilizzo o godimento personale della provvista illecita, in linea con l'assunto per cui tali ipotesi costituiscono la naturale prosecuzione del reato-base (il c.d. post factum non punibile).
La nuova disciplina incontra l'interesse di SAN MARCO poiché è stato inserito tra i reati presupposto della responsabilità amministrativa degli enti ai sensi del Decreto legislativo n. 231/2001 (art. 25-octies).
Le nuove previsioni sono oggetto a tutt'oggi di un vivace dibattito dottrinale, in assenza di applicazioni giurisprudenziali significative, dal momento che la portata applicativa delle stesse appare a molti piuttosto vasta, consentendo di introdurre de facto molte fattispecie finora escluse dalla qualifica di reato presupposto.
A titolo di esempio possiamo indicare che, sulla scorta di alcuni orientamenti della giurisprudenza in tema di riciclaggio, se il reato tributario dell'infedele dichiarazione è compiuto dall'amministratore nell'interesse della società, il risparmio di imposta si confonde nel patrimonio sociale e quindi si configura in via automatica il reimpiego in attività economica. Pertanto, se questa impostazione dovesse essere confermata anche in materia di autoriciclaggio, l'amministratore autore della dichiarazione infedele potrebbe essere chiamato a rispondere anche per l'autoriciclaggio, ad esempio, per aver pagato i dipendenti con la provvista illecita, anche laddove non si sia attivato per far perdere la traccia del collegamento tra il delitto-base e l'utilità.
L'azienda auspica che che non si incorra in imputazioni automatiche per autoriciclaggio e che si dia seguito alle intenzioni del legislatore, richiamate anche da una parte della dottrina, interpretando con rigore l'art. 648-ter.1 e, quindi, valorizzando l'elemento più caratterizzante delle condotte di riciclaggio, vale a dire l'idoneità a nascondere la natura illecita dei proventi. Questo approccio consentirebbe, infatti, di escludere la configurazione in concreto dell'autoriciclaggio nei casi in cui non è possibile identificare e isolare dal patrimonio del contribuente il provento illecito oggetto delle successive operazioni di reimpiego, sostituzione o trasferimento.
(Fonti: Istituto di Studi sulla Responsabilità Amministrative degli Enti. Circolare n. 19867 Confindustria)
Tenuto conto degli orientamenti che si profilano, Il Modello Organizzativo di SAN MARCO ha inserito il nuovo reato fra i presupposti della responsabilità e ha adeguato le relative previsioni di rischio per le attività sensibili che possono risultare interessate dalle disposizioni di legge, aumentando le pene relative.
Le sessioni di audit per verificare la concreta pericolosità delle attività stesse dovranno essere svolte nel corso del 2017 - 2018, e verranno opportunamente

documentate nei progressivi verbali, e relazionate nel report finale dello stesso anno.

Sanzioni previste

L'art. 648 ter 1 punisce con la pena della reclusione da due a otto anni e la multa da euro 5.000 a euro 25.000 chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.
Al secondo comma si prevede una cornice edittale più tenue - reclusione da uno a quattro anni e multa da 2.500 a 12.500 euro - se il delitto non colposo presupposto è punito con la reclusione non superiore nel massimo a cinque anni. Tornano invece ad applicarsi le più severe pene di cui al primo comma se si tratta di delitto commesso con le condizioni e le modalità di cui all'art. 7 del Decreto Legge n. 152 del 1991, convertito dalla Legge n. 203 del 1991, che contempla l'aggravante del c.d. metodo e fine dell'agevolazione mafiosa.
Al quarto comma si stabilisce invece una causa di non punibilità per «le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale».
La disposizione si chiude con la previsione di una circostanza aggravante allorché i fatti sono commessi nell'esercizio di attività bancaria o finanziaria o di altra attività professionale e con una diminuzione rilevante di pena - fino alla metà - nel caso l'autore «si sia efficacemente adoperato per e vitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto».
Il quarto comma dell'art. 648 ter 1 c.p. stabilisce che «fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale»6. Tale previsione sembra definire in negativo i contorni della fattispecie: da un lato, l'area della rilevanza penale segnata dall'impiego in attività economiche, finanziarie, imprenditoriali o speculative, dall'altro, l'area della non punibilità costituita dal mero utilizzo o godimento personale.

La responsabilità 231 per i fatti di autoriciclaggio

Con l’inserimento del nuovo delitto di autoriciclaggio all’interno dell’art. 25 octies, e posto che ogni «delitto non colposo» produttivo di un provento può costituire il

reato-presupposto del delitto di autoriciclaggio, la teorica espansione della responsabilità da reato dell'ente, ricorrendone ovviamente tutte le altre condizioni previste dal D.Lgs. 231/2001 deve essere temperata dall'applicazione rigorosa dei principi di legalità e tassatività.
In particolare, per potersi configurare responsabilità dell'ente ai sensi del D.Lgs. 231/2001 per il reato di autoriciclaggio, appare necessario che:
1. un soggetto apicale o subordinato commetta o concorra a commettere un delitto non colposo produttivo di un provento, presumibilmente (ma non necessariamente) nell'interesse o a vantaggio dell'ente; quest'ultimo ne sarà responsabile ai sensi del D.Lgs. 231 /2001 solo se ciò sia espressamente previsto da detto Decreto.
2. lo stesso soggetto poi impieghi, sostituisca o trasferisca (in attività economiche, finanziarie, imprenditoriali o speculative) quel provento (in ciò concretandosi la condotta di autoriciclaggio) «nell'interesse o a vantaggio» dell'ente (che quindi abbia la disponibilità o tragga vantaggio dall'utilizzo dei proventi del delitto non colposo commesso dal proprio soggetto apicale o dal dipendente), "in modo da ostacolare concretamente l'identificazione della provenienza delittuosa" del provento medesimo. È dubbio peraltro che l'art. 25 octies possa essere interpretato nel senso di escludere la rilevanza, ai fini della configurabilità dell'illecito amministrativo dell'ente, di condotte che abbiano a oggetto proventi di reati non previsti nell'elenco dei reati presupposto8.
È comunque essenziale la funzione selettiva, sia ai fini della responsabilità penale del soggetto agente, che della responsabilità amministrativa dell'ente, svolta dal requisito del concreto ostacolo alla provenienza delittuosa: esso dovrà essere puntualmente riscontrato, per evitare il rischio di punire per autoriciclaggio anche operazioni di reimpiego delle utilità illecite prive di quell'ulteriore disvalore penale che fonda la punibilità del reato di cui all'art. 648 ter1 c.p. In altri termini, sarà necessario accertare la sussistenza di condotte dissimulatorie ovvero anomale rispetto all'ordinaria attività mentre semplici operazioni "tracciabili", non avendo tali caratteristiche, non dovrebbero assumere rilevanza penale; diversamente si priverebbe di significato la precisa scelta del legislatore di esigere una idoneità 'qualificata' dell'operazione a impedire la ricostruzione della provenienza delittuosa del denaro, dei beni e della utilità che sono oggetto.
3. Il reato di autoriciclaggio sussiste nelle ipotesi in cui le relative condotte siano successive al perfezionamento del reato che ha dato origine ai proventi illeciti, anche se compiute dopo la sua estinzione (ad es. per prescrizione), o anche se l'autore del medesimo non sia imputabile o punibile, oppure manchi una condizione di procedibilità (ad es., per difetto di querela, oppure di richiesta del Ministro della Giustizia, necessaria per perseguire i reati comuni commessi all'estero, ai sensi degli artt. 9 e 10 c.p.).
Le attività sub 2) erano già punibili, peraltro, a titolo di riciclaggio o reimpiego, con conseguente possibile responsabilità dell'ente, ad eccezione però dei casi in cui ad agire fosse l'autore o concorrente nel delitto presupposto, situazione oggi coperta dall'art. 648 ter 1 c.p.
(Fonte: Circolare ABI n. 6 del 1 Dicembre 2015)

Condotte punibili

L'autoriciclaggio (al pari del riciclaggio) è un reato a forma libera, che può essere integrato da qualsiasi condotta idonea ad ostacolare concretamente l'identificazione della provenienza delittuosa del bene impiegato, sostituito ovvero trasferito, in attività economiche, finanziarie, imprenditoriali o speculative.
In questa prospettiva possono essere utili le osservazioni già svolte dalla giurisprudenza di legittimità con riguardo al riciclaggio: è stato infatti osservato dalla Suprema Corte (es., Cass. Sez. IV del 23.3.2000) che le condotte devono essere concretamente idonee a dissimulare la provenienza delittuosa del bene con la conseguenza di impedire, tra l'altro, possibili iniziative investigative. Rilevano in questo ambito anche tutte quelle attività volte a ostacolare la segnalazione di operazione sospetta ai sensi dell'art. 41 del D.Lgs. 231/2007, con la conseguenza che appaiono sempre più legate la disciplina penale (rectius artt. 648-bis, 648-ter, 648-ter.1) e la disciplina dei presidi antiriciclaggio che ha dato applicazione alla III Direttiva.
Ciò posto, in giurisprudenza sono state individuate talune condotte che, pur essendo calibrate sul reati di cui agli artt.648-bis e 648-ter c.p., a mio avviso possono comunque essere applicabili anche al reato di autoriciclaggio. Segnatamente:

- integra il reato di riciclaggio il compimento di operazioni volte non solo ad impedire in modo definitivo, ma anche a rendere difficile l'accertamento della provenienza del denaro, dei beni o delle altre utilità, attraverso un qualsiasi espediente che consista nell'aggirare la libera e normale esecuzione dell'attività posta in essere (ex plurimis, Cass. 2818/2006; Cass. 16980/2007);
- il semplice trasferimento di danaro di provenienza illecita da un conto corrente a un altro integra gli estremi del reato di riciclaggio, essendo sufficiente a tal proposito il solo dolo eventuale. Il delitto di riciclaggio è infatti configurabile attraverso un "qualsiasi prelievo o trasferimento di fondi successivo a precedenti versamenti o anche con un mero trasferimento di denaro di provenienza da un conto corrente bancario a un altro diversamente intestato, e acceso presso un differente istituto di credito" ovvero anche tra conti correnti accesi presso lo stesso istituto di credito;
- integra di per sé un autonomo atto di riciclaggio, essendo il reato di cui all'art. 648- bis c.p. a forma libera e potenzialmente a consumazione prolungata, attuabile anche con modalità frammentarie e progressive, qualsiasi prelievo o trasferimento di fondi successivo a precedenti versamenti, ed anche il mero trasferimento di denaro di provenienza delittuosa da un conto corrente bancario ad un altro diversamente intestato, ed acceso presso un differente istituto di credito. (Fattispecie in cui è stata ritenuta penalmente rilevante l'operazione di svuotamento della cassa di un gruppo societario ed il successivo trasferimento del denaro ad un soggetto, attraverso assegni circolari e bonifici, con l'incarico di reimpiegare le somme per finanziare altra società - Cass, Sez. II, 43881/2014);

- integra il delitto di riciclaggio la sostituzione, con denaro, di documenti fiscali provenienti dal delitto di cui all'art. 8, D.Lgs. 10.3.2000, n. 74 (Cass., Sez. II, 17.5.2013, n. 29452);
- commette il delitto colui che accetta di essere indicato come beneficiario economico di conti correnti accesi all'estero, formalmente intestati a società aventi sede in paradisi fiscali, ma in realtà appartenenti a terzi, e sui quali confluiscono i proventi di attività delittuosa (Cass., Sez. VI, 22.5.2013, n. 24548).

A seguito dell'evoluzione normativa delle fattispecie del codice penale e della disciplina penal-tributaria, il rapporto tra la disciplina antiriciclaggio e il fenomeno dell'evasione fiscale è ancora più stretto, in ragione dell'indubbio arricchimento (in termini sia di elementi informativi acquisibili, sia di strumenti di contrasto) assicurato dal sistema antiriciclaggio alla lotta contro i fenomeni evasivi, soprattutto se connotati da elevata insidiosità.
In questa prospettiva, secondo l'insegnamento della Suprema Corte, i delitti dichiarativi e di emissione di fatture fittizie possono sicuramente essere reati presupposto dell'autoriciclaggio, poiché nel concetto di "altre utilità" ben si può ricomprendere il risparmio di spesa che l'agente ottiene evitando di pagare le imposte dovute anche se commesso all'estero.
Non è un caso, infatti, che la costante giurisprudenza della Suprema Corte ritiene che costituisca profitto dei reati tributari la somma corrispondente all'imposta evasa, sicché, ai sensi della Legge Finanziaria n. 244 del 2007, art. 1, comma 143, se ne ammette il sequestro preventivo finalizzato alla successiva confisca.
Di conseguenza è assolutamente evidente che chi commette un reato tributario oggi potrebbe vedersi perseguito anche per autoriciclaggio, qualora occulti o reimpieghi i proventi dell'evasione; specularmente, a carico di società potrebbero trovare applicazione tanto le sanzioni tributarie quanto le rischiosissime sanzioni "231/2001". Posto che, come noto, la legge n. 186/2014 inserisce l'autoriciclaggio anche nell'elenco dei reati presupposto della responsabilità degli enti disciplinata dal D.Lgs. n. 231/2001.
Ma proprio in relazione a quest'ultime Confindustria segnala che tale scelta del legislatore rende particolarmente severa la risposta sanzionatoria (con dubbi di compatibilità con il principio ordinamentale del ne bis in idem – Corte europea dei diritti dell'uomo del 4.3.2014), in quanto per i reati tributari si cumulerebbero le seguenti sanzioni:
- amministrativa;
- penale per il reato base;
- penale per l'autoriciclaggio;
- amministrativa ai sensi del Decreto 231, a carico dell'impresa.

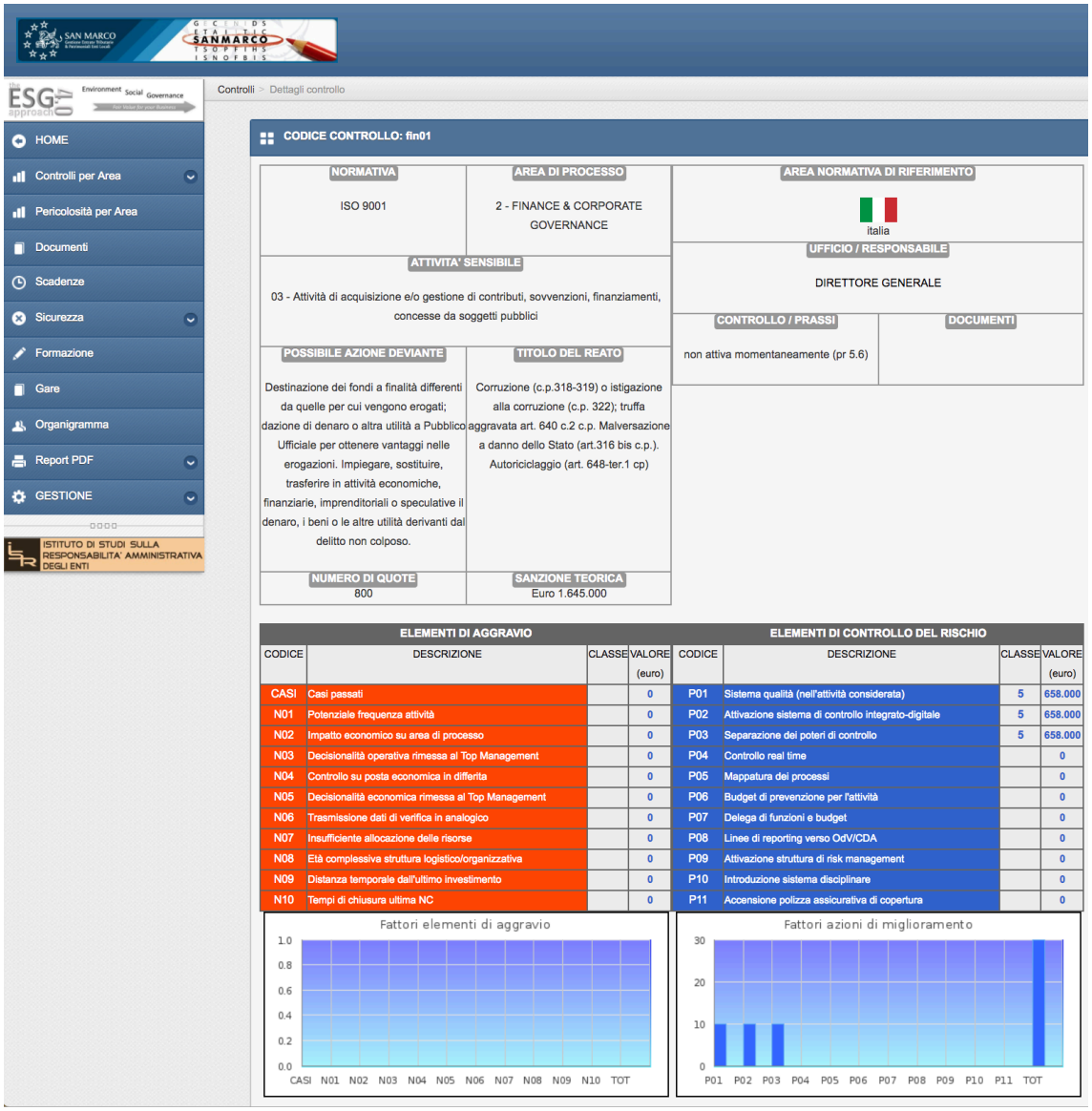
(Fonte: Giovanni Barbato, Commento alla Circolare n. 19867 di Confindustria)

La prevenzione del reato di Autoriciclaggio in SAN MARCO

Adeguamento delle schede di controllo del sistema Cloudgovernance ®

Le schede di controllo già implementate per l'analisi del rischio degli altri reati presupposto sono state revisionate nella struttura, comprendendo le sanzioni indicate dalla normativa introdotta in tema di autoriciclaggio.
Le ipotesi di sanzione misurate con lo strumento dinamico risultano quindi proporzionalmente aumentate di gravità, nella misura in cui la fase di audit abbia rilevato un pericolo di commissione dei reati presupposto che possono portare ad una condotta tipica di autoriciclaggio.

Esempio di scheda di controllo con indicazione del reato di autoriciclaggio



Indicatori di rischio

Alcuni esempi di indicatori di rischio con riferimento a operazioni ovvero flussi in entrata e in uscita “sospetti”:

- pagamento agli amministratori di emolumenti non deliberati ovvero deliberati, ma in misura sproporzionata all’attività;
- pagamenti ai parenti degli amministratori per non meglio precisate attività di consulenza;
- pagamento di compensi agli amministratori a titolo di consulenza;
- pagamento di consulenze a società che si trovano in paesi black list o off-shore;
- pagamenti effettuati per attività svolte da controparti italiane, ma accreditate su conti correnti di società in paesi black list o off-shore;
- aumenti di capitale effettuati da società con sedi in paesi black list o off-shore;
- finanziamenti soci provenienti da società fiduciarie o esterovestite;
- finanziamenti soci ricorrenti anche da parte di una società del gruppo partecipante o controllante senza una sottostante ragione di ordine imprenditoriale e reiterati prelievi a titolo di rimborso finanziamento soci non deliberati dal CdA;
- movimentazione eccessiva del conto di cassa senza una descrizione analitica delle operazioni compiute nel mastrino di cassa o nel libro giornale;
- sponsorizzazioni o donazioni per importi sensibili a Fondazioni o Onlus non meglio individuate;
- operazioni di significativo ammontare in assenza di motivazioni correlate al proprio business;
- operazioni ripetute e di ammontare significativo effettuate in contropartita con società che risultano create di recente e hanno un oggetto sociale generico o incompatibile con il business della società;
- stipula di rapporti contrattuali con vincoli o pegni a favore di terzi che non presentano alcun collegamento con la società;
- acquisto di un ingente ammontare di strumenti finanziari a elevata liquidità seguito dalla richiesta di prestiti garantiti dagli stessi strumenti finanziari;
- frequenti operazioni di investimento a lungo termine in strumenti finanziari immediatamente seguite dalla richiesta di liquidare la posizione e di trasferire i relativi proventi

Generalità dei reati inerenti la criminalità organizzata

Con la Legge n. 94 del 23 luglio 2009, recante disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia (c.d. Legge Sicurezza Pubblica) il legislatore italiano ha disposto modifiche al decreto legislativo 231/2001. In conseguenza, dopo l'art. 24-bis relativo ai delitti informatici, è stato inserito l'art. 24-ter in materia di delitti di criminalità organizzata.
L'inserimento dei delitti contro la criminalità organizzata tra i reati presupposto previsti dal d.lgs. 231/01 risale all'applicazione dell'art. 10 della legge 146/2006 "Ratifica della Convenzione ONU sulla lotta alla criminalità organizzata transnazionale" aveva già previsto alcuni delitti associativi tra i reati presupposto nel caso in cui tali reati avessero carattere transnazionale. Tale introduzione ed estensione anche all'ambito nazionale risponde all'esigenza di rafforzare la lotta contro la criminalità di impresa.

Art. 24-ter. - (Delitti di criminalità organizzata).
1. In relazione alla commissione di taluno dei delitti di cui agli articoli 416, sesto comma, 416- bis, 416-ter e 630 del codice penale, ai delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonchè ai delitti previsti dall'articolo 74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, si applica la sanzione pecuniaria da quattrocento a mille quote.
2. In relazione alla commissione di taluno dei delitti di cui all'articolo 416 del codice penale, ad esclusione del sesto comma, ovvero di cui all'articolo 407, comma 2, lettera a), numero 5), del codice di procedura penale, si applica la sanzione pecuniaria da trecento a ottocento quote. 3. Nei casi di condanna per uno dei delitti indicati nei commi 1 e 2, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore ad un anno.
4. Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati nei commi 1 e 2, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'articolo 16, comma 3.
Il nuovo articolo 24-ter del d.lgs. 231/2001 presenta, quindi, due diverse tipologie di delitti di criminalità organizzata con trattamento sanzionatorio differenziato.

La tipologia dei reati di criminalità organizzata (art. 24- ter del decreto legislativo 231/2001).

Si riporta di seguito una breve descrizione dei reati contemplati nell'art. 24-ter del Decreto 231 la cui commissione possa comunque comportare un interesse e/o un vantaggio per la Società.

ART. 416 C.P. ASSOCIAZIONE PER DELINQUERE

Quando tre o più persone si associano allo scopo di commettere più delitti, coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, per ciò solo, con la reclusione da tre a sette anni. Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni. I capi soggiacciono alla stessa pena stabilita per i promotori. Se gli associati scorrono in armi le campagne o le pubbliche vie, si applica la reclusione da cinque a quindici anni. La pena è aumentata se il numero degli associati è di dieci o più. Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, nonché all'articolo 12, comma 3-bis, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, si applica la reclusione da cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma.

ART. 416 BIS C.P. ASSOCIAZIONI DI TIPO MAFIOSO ANCHE STRANIERE

Chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone, è punito con la reclusione da sette a dodici anni. Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da nove a quattordici anni. L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali. Se l'associazione è armata si applica la pena della reclusione da nove a quindici anni nei casi previsti dal primo comma e da dodici a ventiquattro anni nei casi previsti dal secondo comma. L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito. Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti, le pene stabilite nei Modello di organizzazione, gestione e controllo commi precedenti sono aumentate da un terzo alla metà. Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servirono e furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego. Le disposizioni del presente articolo si applicano anche alla camorra, alla 'ndrangheta e alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.

ART. 416 TER SCAMBIO ELETTORALE POLITICO-MAFIOSO

La pena stabilita dal primo comma dell'articolo 416 bis si applica anche a chi ottiene la promessa di voti prevista dal terzo comma del medesimo articolo 416 bis in cambio di erogazione di denaro. Le norme in esame riguardano la criminalità organizzata, fenomeno che provoca un elevato allarme sociale nella collettività a causa della maggiore potenzialità delinquenziale delle organizzazioni rispetto al singolo autore di reato, ovvero della maggiore pericolosità del programma criminoso dell'organizzazione rispetto al disegno criminoso del singolo individuo.
Le fattispecie di cui sopra si riferiscono alla semplice partecipazione, nonché alla promozione, direzione, costituzione, organizzazione di un'associazione, composta da tre o più persone e dotata, anche in minima parte, di una "strutturazione" (divisione di compiti, gerarchie etc.), e di "stabilità" che permettono di distinguerla dal semplice concorso di persone nel reato, caratterizzato, invece, dall'occasionalità e accidentalità dell'accordo criminoso. Lo scopo dell'associazione deve essere, anche se non unico e prevalente, quello di realizzare un programma criminoso, cioè la commissione di uno o più reati.

Lo schema applicativo dell'art. 24 ter

L'art. 24 ter, con una formulazione non troppo lineare, riferendosi genericamente ai reati di cui all'art. 416 c.p., considera come "ipotesi base" la commissione, in forma organizzata di qualsiasi delitto, ad esclusione di quelli, ritenuti più gravi, di cui all'art. 416 c. 6 c.p. (v. appresso), nonché dei delitti previsti dal 407 c. 2 lett. a) n. 5 c.p.p. (delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110).
Lo stesso articolo 24 ter, prevede poi, alcune "ipotesi aggravate" di "reato/i-fine" rispetto all'ipotesi base:
- richiamando l'art. 416 c. 6 c.p., include tra queste la commissione in forma associata dei reati di:
• Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)
• Tratta di persone (art. 601 c.p.)
• Acquisto e alienazione di schiavi (art. 602)
• Promozione, direzione, organizzazione, finanziamento del trasporto, o il trasporto stesso, di stranieri nel territorio dello Stato in violazione delle norme contro l'immigrazione clandestina, ovvero compie altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente, in presenza di due o più delle seguenti condizioni:
a) il fatto riguarda l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone;

b) la persona trasportata è stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale;
c) la persona trasportata è stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale;
d) il fatto è commesso da tre o più persone in concorso tra loro o utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti;
e) gli autori del fatto hanno la disponibilità di armi o materie esplodenti.
- richiamando gli articoli 416 bis, 416 ter e 630 c.p. si riferisce alla commissione in forma associata dei reati di:
• Associazioni di tipo mafioso anche straniere • Scambio elettorale politico-mafioso
• Sequestro a scopo di rapina o di estorsione
- richiamando (i delitti di cui al)l'art. 74 del D.P.R. n. 309/1990 si riferisce alla:
• Associazione finalizzata al traffico di sostanze stupefacenti o psicotrope

Altre ipotesi aggravate a cui fa riferimento l'art. 24 ter sono quelle in cui i delitti (qualsiasi delitto) vengano commessi in forma associata avvalendosi della forza di intimidazione del sodalizio di tipo mafioso e della condizione di assoggettamento e di omertà che ne deriva, e quella in cui i delitti medesimi vengano commessi al fine di agevolare l'attività delle associazioni di tipo mafioso.
Modello di organizzazione, gestione e controllo
E' opportuno precisare che è associazione di tipo mafioso quella in cui, coloro che ne fanno parte, si avvalgono della forza intimidatrice e della condizione di assoggettamento e di omertà che ne deriva, per commettere delitti, nonché per acquisire in modo diretto o indiretto la gestione o il controllo di attività economiche, concessioni, autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti ovvero impedire il libero esercizio del voto o di procurare voti a sè o ad altri. E' punita, inoltre, la condotta di chi agevola l'attività delle associazioni di tipo mafioso o ottiene la promessa di voti in cambio di erogazione di denaro. Le disposizioni dell'articolo 416 bis si applicano anche alla camorra, alla 'ndrangheta e alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso.

La Legge n. 94 del 23 luglio 2009, recante disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia (c.d. Legge Sicurezza Pubblica) ha disposto modifiche al decreto legislativo 8 giugno 2001, n. 231. In particolare, dopo l'art. 24-bis relativo ai delitti informatici, è stato inserito l'art. 24-ter in materia di delitti di criminalità organizzata.
L'inserimento dei delitti contro la criminalità organizzata tra i reati presupposto previsti dal d.lgs. 231/01 non rappresenta una novità assoluta. Infatti, l'art. 10 della legge 146/2006 "Ratifica della Convenzione ONU sulla lotta alla criminalità organizzata transnazionale" aveva già previsto alcuni delitti associativi tra i reati presupposto nel caso in cui tali reati avessero carattere transnazionale. Tale

introduzione ed estensione anche all'ambito nazionale risponde all'esigenza di rafforzare la lotta contro la criminalità di impresa.

Principali attività a rischio di commissione dei reati

Lo scopo di questa Parte Speciale è di definire canoni comportamentali volti a disciplinare aspetti propri della gestione caratteristica per i quali, tramite attività di risk assessment, sono stati rilevati potenziali profili di rischiosità in relazione al dettato del D.Lgs. 231/01. In particolare, si fa riferimento a quanto previsto dal Decreto in relazione alle seguenti tipologie di attività:
- Approvvigionamento di beni e servizi e inserimento anagrafiche fornitori nel sistema;
- Gestione delle attività amministrativo-contabili e dei pagamenti relativi ad approvvigionamento di beni e servizi;
- Gestione contratti di appalto e inserimento anagrafiche clienti nel sistema;
- Gestione delle attività amministrativo-contabili e degli incassi relativi al ciclo attivo;
- Attività di dismissione dei cespiti aziendali e relativi adempimenti amministrativo-contabili e di incasso;
- Operazioni su quote di capitale sociale e altre operazioni straordinarie e di quelle di acquisto/vendita di strumenti finanziari; Modello di organizzazione, gestione e controllo
- Gestione del personale: dipendenti, agenti e rappresentanti, consulenti e altri collaboratori esterni e relativi adempimenti amministrativo-contabili e di pagamento;
- Attività di sponsorizzazione e gestione di eventi.

Le Leggi che regolano questa materia prevedono sanzioni penali per chiunque ne trasgredisca la lettera e lo spirito. Tra gli specifici presidi di controllo che l'azienda deve adottare per esimersi dalla responsabilità per i nuovi reati con finalità associativa (art. 24-ter), si deve tenere conto che il rischio maggiore è rappresentato dalla "controparte": in concreto, la principale attività di prevenzione per questo categoria di reati è rappresentata dalla verifica che la persona fisica o giuridica con la quale la Società intrattiene rapporti commerciali sia in possesso di adeguati requisiti di professionalità e di onorabilità.
Particolare attenzione viene data alla stipula di contratti ed al puntuale ed effettivo svolgimento di prestazioni concordate in conformità delle leggi vigenti. E' necessario verificare l'affidabilità dei fornitori e delle parti terze con i quali SAN MARCO intrattiene rapporti di fornitura di tali servizi. Particolare attenzione dovrà essere posta alla stipula dei contratti ed al puntuale ed effettivo svolgimento delle prestazioni concordate in conformità alle leggi vigenti.

Destinatari della parte speciale – principi generali di comportamento nelle aree di attività a rischio

Questa Parte Speciale si riferisce a comportamenti posti in essere da Amministratori, Dirigenti e Dipendenti della Società nelle aree di attività a rischio, nonché da Collaboratori, Consulenti e Partners con essa operanti sulla base di un rapporto contrattuale, anche temporaneo (qui di seguito, tutti denominati "Destinatari").
Al fine di individuare l'ownership dei processi svolti nelle aree sensibili, tutti i Destinatari sono considerati "responsabili" per ogni singola operazione a rischio da loro direttamente compiuta o comunque effettuata nell'ambito della funzione di loro riferimento.
La presente Parte Speciale ha l'obiettivo di disciplinare la condotta dei Destinatari affinché adottino comportamenti conformi a quanto previsto nel Modello Organizzativo, al fine di impedire il verificarsi dei reati contemplati nel Decreto.
Quanto premesso, tra gli attori coinvolti nei processi di gestione e monitoraggio nelle aree sensibili si rilevano:
• Presidente;
• Consiglio di Amministrazione;
• Direzione Generale;
• Responsabile Area Amministrativa;
• Responsabile Area Acquisti;
• Responsabile Qualità;
• Collaboratori esterni.
Rimane inteso che tutti i soggetti interni ed esterni alla Società, quali che siano tipo e livello della loro collaborazione, sono tenuti alla stretta osservanza di quanto prescritto nel Modello. In linea generale, è espressamente vietato agli organi societari e ai dipendenti della Società (nonché ai Consulenti ed i Partner nella misura necessaria alle funzioni dagli stessi svolte):
- porre in essere, promuovere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato tra quelle considerate nelle presente sezione (art. 24-ter e art. 25-novies del D.Lgs. 231/2001);
- utilizzare stabilmente l'ente o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei Reati di cui alla presente sezione;
- promuovere, costituire, organizzare o dirigere associazioni che si propongono il compito di atti di violenza con fini illeciti;
- assumere commesse, fornire prodotti o effettuare qualsivoglia operazione commerciale e/o finanziaria, sia in via diretta che per il tramite di interposta persona, con soggetti – persone fisiche o persone giuridiche - i cui nominativi siano stati segnalati dalle autorità europee e internazionali preposte alla prevenzione dei Reati di associazione a delinquere;
- effettuare operazioni o assumere commesse ritenute anomale per tipologia o oggetto ed instaurare o mantenere rapporti che presentano profili di anomalia; effettuare prestazioni in favore delle società di servizi, dei Consulenti e dei

Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi; Modello di organizzazione, gestione e controllo
- riconoscere compensi in favore delle società di servizi, dei Consulenti e dei Partner che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale.

Principi di attuazione dei comportamenti descritti

Al fine dell'efficace attuazione di quanto sopra riportato, i dipendenti, gli organi societari (nonché i Consulenti ed i Partner nella misura necessaria alle funzioni dagli stessi svolte) operano in base a procedure che consentono quanto segue:
- i dati raccolti relativamente ai rapporti con clienti, Consulenti e Partner devono essere completi ed aggiornati, sia per la corretta e tempestiva individuazione dei medesimi sia per una valida valutazione del loro profilo;
- la gestione anomala dei rapporti sia preventivamente rilevata e tempestivamente rifiutata e gli indici di anomalia predefiniti siano in grado di selezionare tale anomalia.
- forniture a prezzi/ condizioni generali palesemente non allineate agli standard di mercato, determinabili secondo la normale diligenza devono essere segnalate all'OdV;
- raccolta di informazioni sul fornitore che consentano di valutare in modo più completo il profilo reputazionale della controparte. Tali verifiche possono anche essere affidate a strutture esterne alla Società;
- visite in loco presso le unità produttive del fornitore volte a valutare la capacità di fornire beni che rispettino gli standard qualitativi richiesti e le specifiche di Legge applicabili;

Compiti dell'Organismo di vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'art. 24 ter del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso. I compiti di

vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'art. 24 ter del D. Lgs. n. 231/2001 del Decreto sono i seguenti:
- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cui all'art. 24 ter del Decreto;
- proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei delitti connessi ai reati di criminalità organizzata di cui alla presente Parte Speciale;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- conservare traccia dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti.

Qualora fossero accertate dall'OdV violazioni del Modello Organizzativo, ivi comprese le specifiche procedure adottate, lo stesso Organismo di Vigilanza informa di ciò, senza indugi, il Consiglio di Amministrazione e il Collegio Sindacale, qualora nominato.

Parte Speciale 4:

Reati di omicidio colposo e lesioni personali colpose derivanti da inosservanza di norme poste a tutela della salute e sicurezza dei lavoratori.

Reati Contro la Personalità Individuale

Il significato del D.Lgs. 81/08 nel sistema organizzativo di SAN MARCO .

La terza parte speciale del modello organizzativo di SAN MARCO riguarda il reato recentemente incluso fra quelli che possono determinare la responsabilità amministrativa dell'ente ai sensi del D.Lgs. 231/01. Inoltre il D.Lgs. 81/08 contempla la necessità che il datore di lavoro adotti ed attui efficacemente un modello organizzativo idoneo alla prevenzione dei reati inerenti alla sicurezza sul lavoro.
SAN MARCO oltre ad avere una tradizione di rispetto per la salute e la sicurezza nei luoghi di lavoro che risale alla propria stessa nascita, si è sempre resa adempiente alle normative che si sono via via susseguite, elaborando opportunamente i documenti di valutazione dei rischi richiesti dal D.Lgs. 81/08 e successive modificazioni.
I documenti di valutazione dei rischi e l'altra documentazione richiesta ed allegata vengono acclusi e considerati parte integrante del presente modello organizzativo, e vengono di seguito riportati.

Il contenuto delle nuove norme

Il 9 aprile 2008 il Presidente della Repubblica ha firmato il nuovo D.Lgs. 81/08 recante “attuazione dell’art. 1 della legge 3 agosto 2007 n. 123 in materia di tutela della salute e sicurezza nei luoghi di lavoro”, testo che introduce finalmente nel nostro ordinamento un “corpus” normativo destinato a sostituire la precedente disciplina in materia, assumendo la veste di un vero e proprio Testo Unico non meramente compilativo.
Si è trattato di un lavoro lungo e complesso che riordina la materia, innova sul piano della prevenzione, della formazione, del potenziamento e del coordinamento della vigilanza, del ruolo delle parti sociali e dei rappresentanti dei lavoratori per la sicurezza e della diffusione della cultura della sicurezza, assicurando un sistema sanzionatorio equilibrato.

Senza alcun dubbio il nuovo decreto si caratterizza per un generalizzato inasprimento sanzionatorio, resosi necessario, nelle intenzioni dell'Esecutivo, per garantire maggior spazio applicativo alla disciplina in tema di prevenzione infortuni, considerato il desolante quadro emergente dalle statistiche annuali in tema di infortuni negli ambienti di lavoro.
Le prime innovazioni che si incontrano nel D.Lgs. 81/08 riguardano le definizioni: fra le più importanti aggiunte rispetto al passato si segnalano quelle di "dirigente" e di "preposto", figure centrali per la gestione della sicurezza negli ambienti di lavoro, i cui elementi distintivo sono tratti dalla Giurisprudenza in materia; degne di nota la definizione di "salute", corrispondente alla definizione dell'Organizzazione Mondiale della Sanità, e finalmente ricomprendente anche la sindrome da stress, la definizione di "norma tecnica", nonché di "buone prassi" e di "responsabilità sociale delle imprese", questi ultimi considerati dall'art. 1, comma 2, lett. l) del citato Decreto, come elementi fondamentali per orientare i comportamenti dei datori di lavoro e migliorare i livelli di tutela definiti legislativamente[1].

[1]Il testo del Decreto:
Art. 2.Definizioni
1. Ai fini ed agli effetti delle disposizioni di cui al presente decreto legislativo si intende per:
a) «lavoratore»: persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione di un datore di lavoro pubblico o privato, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione, esclusi gli addetti ai servizi domestici e familiari. Al lavoratore cosi' definito e' equiparato: il socio lavoratore di società o di societa', anche di fatto, che presta la sua attività per conto delle societa' e dell'ente stesso; l'associato in partecipazione di cui all'articolo 2549, e seguenti del codice civile; il soggetto beneficiario delle iniziative di tirocini formativi e di orientamento di cui all'articolo 18 della legge 24 giugno 1997, n. 196, e di cui a specifiche disposizioni delle leggi regionali promosse al fine di realizzare momenti di alternanza tra studio e lavoro o di agevolare le scelte professionali mediante la conoscenza diretta del mondo del lavoro; l'allievo degli istituti di istruzione ed universitari e il partecipante ai corsi di formazione professionale nei quali si faccia uso di laboratori, attrezzature di lavoro in genere, agenti chimici, fisici e biologici, ivi comprese le apparecchiature fornite di videoterminali limitatamente ai periodi in cui l'allievo sia effettivamente applicato alla strumentazioni o ai laboratori in questione; il volontario, come definito dalla legge 1° agosto 1991, n. 266; i volontari del Corpo nazionale dei vigili del fuoco e della protezione civile; il volontario che effettua il servizio civile; il lavoratore di cui al decreto legislativo 1° dicembre 1997, n. 468, e successive modificazioni;
b) «datore di lavoro»: il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilita' dell'organizzazione stessa o dell'unita' produttiva in quanto

esercita i poteri decisionali e di spesa. Nelle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, per datore di lavoro si intende il dirigente al quale spettano i poteri di gestione, ovvero il funzionario non avente qualifica dirigenziale, nei soli casi in cui quest'ultimo sia preposto ad un ufficio avente autonomia gestionale, individuato dall'organo di vertice delle singole amministrazioni tenendo conto dell'ubicazione e dell'ambito funzionale degli uffici nei quali viene svolta l'attività, e dotato di autonomi poteri decisionali e di spesa. In caso di omessa individuazione, o di individuazione non conforme ai criteri sopra indicati, il datore di lavoro coincide con l'organo di vertice medesimo;
c) «azienda»: il complesso della struttura organizzata dal datore di lavoro pubblico o privato;
d) «dirigente»: persona che, in ragione delle competenze professionali e di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attua le direttive del datore di lavoro organizzando l'attività lavorativa e vigilando su di essa;
e) «preposto»: persona che, in ragione delle competenze professionali e nei limiti di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende alla attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa;
f) «responsabile del servizio di prevenzione e protezione»: persona in possesso delle capacita' e dei requisiti professionali di cui all'articolo 32 designata dal datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi;
g) «addetto al servizio di prevenzione e protezione»: persona in possesso delle capacita' e dei requisiti professionali di cui all'articolo 32, facente parte del servizio di cui alla lettera l);
h) «medico competente»: medico in possesso di uno dei titoli e dei requisiti formativi e professionali di cui all'articolo 38, che collabora, secondo quanto previsto all'articolo 29, comma 1, con il datore di lavoro ai fini della valutazione dei rischi ed e' nominato dallo stesso per effettuare la sorveglianza sanitaria e per tutti gli altri compiti di cui al presente decreto;
i) «rappresentante dei lavoratori per la sicurezza»: persona eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro;
l) «servizio di prevenzione e protezione dai rischi»: insieme delle persone, sistemi e mezzi esterni o interni all'azienda finalizzati all'attività di prevenzione e protezione dai rischi professionali per i lavoratori;
m) «sorveglianza sanitaria»: insieme degli atti medici, finalizzati alla tutela dello stato di salute e sicurezza dei lavoratori, in relazione all'ambiente di lavoro, ai fattori di rischio professionali e alle modalita' di svolgimento dell'attività lavorativa;
n) «prevenzione»: il complesso delle disposizioni o misure necessarie anche secondo la particolarita' del lavoro, l'esperienza e la tecnica, per evitare o diminuire i rischi professionali nel rispetto della salute della popolazione e dell'integrita' dell'ambiente esterno;
o) «salute»: stato di completo benessere fisico, mentale e sociale, non consistente solo in un'assenza di malattia o d'infermita';
p) «sistema di promozione della salute e sicurezza»: complesso dei soggetti istituzionali che concorrono, con la partecipazione delle parti sociali, alla realizzazione dei programmi di intervento finalizzati a migliorare le condizioni di salute e sicurezza dei lavoratori;

q) «valutazione dei rischi»: valutazione globale e documentata di tutti i rischi per la salute e sicurezza dei lavoratori presenti nell'ambito dell'organizzazione in cui essi prestano la propria attività, finalizzata ad individuare le adeguate misure di prevenzione e di protezione e ad elaborare il programma delle misure atte a garantire il miglioramento nel tempo dei livelli di salute e sicurezza;
r) «pericolo»: proprieta' o qualita' intrinseca di un determinato fattore avente il potenziale di causare danni;
s) «rischio»: probabilita' di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione;
t) «unita' produttiva»: stabilimento o struttura finalizzati alla produzione di beni o all'erogazione di servizi, dotati di autonomia finanziaria e tecnico funzionale;
u) «norma tecnica»: specifica tecnica, approvata e pubblicata da un'organizzazione internazionale, da un organismo europeo o da un organismo nazionale di normalizzazione, la cui osservanza non sia obbligatoria;
v) «buone prassi»: soluzioni organizzative o procedurali coerenti con la normativa vigente e con le norme di buona tecnica, adottate volontariamente e finalizzate a promuovere la salute e sicurezza sui luoghi di lavoro attraverso la riduzione dei rischi e il miglioramento delle condizioni di lavoro, elaborate e raccolte dalle regioni, dall'Istituto superiore per la prevenzione e la sicurezza del lavoro (ISPESL), dall'Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro (INAIL) e dagli organismi paritetici di cui all'articolo 51, validate dalla Commissione consultiva permanente di cui all'articolo 6, previa istruttoria tecnica dell'ISPESL, che provvede a assicurarne la piu' ampia diffusione;
z) «linee guida»: atti di indirizzo e coordinamento per l'applicazione della normativa in materia di salute e sicurezza predisposti dai Ministeri, dalle regioni, dall'ISPESL e dall'INAIL e approvati in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano;
aa) «formazione»: processo educativo attraverso il quale trasferire ai lavoratori ed agli altri soggetti del sistema di prevenzione e protezione aziendale conoscenze e procedure utili alla acquisizione di competenze per lo svolgimento in sicurezza dei rispettivi compiti in azienda e alla identificazione, alla riduzione e alla gestione dei rischi;
bb) «informazione»: complesso delle attività dirette a fornire conoscenze utili alla identificazione, alla riduzione e alla gestione dei rischi in ambiente di lavoro;
cc) «addestramento»: complesso delle attività dirette a fare apprendere ai lavoratori l'uso corretto di attrezzature, macchine, impianti, sostanze, dispositivi, anche di protezione individuale, e le procedure di lavoro;
dd) «modello di organizzazione e di gestione»: modello organizzativo e gestionale per la definizione e l'attuazione di una politica aziendale per la salute e sicurezza, ai sensi dell'articolo 6, comma 1, lettera a), del decreto legislativo 8 giugno 2001, n. 231, idoneo a prevenire i reati di cui agli articoli 589 e 590, terzo comma, del codice penale, commessi con violazione delle norme antinfortunistiche e sulla tutela della salute sul lavoro;
ee) «organismi paritetici»: organismi costituiti a iniziativa di una o piu' associazioni dei datori e dei prestatori di lavoro comparativamente piu' rappresentative sul piano nazionale, quali sedi

Uno degli aspetti più importanti da segnalare nella normativa del D.Lgs. 81/08 è quello relativo alla delega di funzioni.
L'istituto era, in precedenza, di mera creazione giurisprudenziale, motivato dall'intento di rendere più semplice all'imprenditore, chiamato ad attuare gli obblighi di sicurezza, l'adempimento dei medesimi mediante ricorso a soggetti dotati di particolare competenza professionale e capacità tecnico – giuridiche.
La Giurisprudenza aveva elaborato un vero e proprio catalogo di requisiti soggettivi ed oggettivi in presenza dei quali una delega poteva considerarsi efficace ed effettiva. Tale riconoscimento non aveva mai avuto seguito legislativo, salvo l'intervento correttivo del D.Lgs. 626/94 che prevedeva in negativo gli adempimenti non delegabili da parte del datore di lavoro.
Il nuovo Testo Unico invece sancisce l'istituto della delega all'art. 16, individuandone i requisiti di natura oggettiva e soggettiva che possono essere così individuati:

- la delega deve risultare da atto scritto recante data certa;
- il delegato deve possedere tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
- la delega deve attribuire al soggetto tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
- la delega deve attribuire al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;
- la delega deve essere accettata per iscritto dal delegato;
- alla delega deve essere data adeguata e tempestiva pubblicità;

Lo stesso testo di legge tuttavia prevede (art. 17) che vi siano alcune funzioni assolutamente non delegabili, e cioè:

- la valutazione dei rischi e la conseguente predisposizione del documento di valutazione dei rischi;

privilegiate per: la programmazione di attività formative e l'elaborazione e la raccolta di buone prassi a fini prevenzionistici; lo sviluppo di azioni inerenti alla salute e alla sicurezza sul lavoro; l'assistenza alle imprese finalizzata all'attuazione degli adempimenti in materia; ogni altra attività o funzione assegnata loro dalla legge o dai contratti collettivi di riferimento;
ff) «responsabilita' sociale delle imprese»: integrazione volontaria delle preoccupazioni sociali ed ecologiche delle aziende e organizzazioni nelle loro attività commerciali e nei loro rapporti con le parti interessate.

- la designazione del soggetto responsabile del servizio di prevenzione e protezione dai rischi.

Un altro aspetto importante introdotto dal Testo Unico è l'obbligo di adozione dei modelli di organizzazione e gestione, previsto all'art. 30.
Tale norma sancisce la definitiva affermazione del concetto di colpa nell'organizzazione, in quanto non è più sufficiente soltanto verificare l'esistenza di una responsabilità penale del trasgressore improntata sui cardini della responsabilità penale dettati dall'art. 27 Cost., ma è necessario valutare il modello organizzativo adottato in via preventiva per impedire il verificarsi di eventi lesivi dell'integrità fisica dei lavoratori ovvero, anche in assenza di eventi lesivi, per mantenere elevati gli standards di sicurezza[2].

[2] Art. 30.Modelli di organizzazione e di gestione
1. Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilita' amministrativa delle persone giuridiche, delle societa' e delle associazioni anche prive di personalita' giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:
a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
d) alle attività di sorveglianza sanitaria;
e) alle attività di informazione e formazione dei lavoratori;
f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.
2. Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.
3. Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonche' un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.
4. Il modello organizzativo deve altresi' prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneita' delle misure

La prevenzione in materia di salute e sicurezza nel modello organizzativo di SAN MARCO

La materia inerente la salute e sicurezza dei lavoratori è stata oggetto di attento esame nello svolgimento della risk analysis, condotto attraverso l'analisi della documentazione fornita dai responsabili della adozione e manutenzione del sistema di controllo della salute e sicurezza nei luoghi di lavoro.
La documentazione, al momento dell'adozione del Modello Organizzativo, presenta le caratteristiche idonee all'adeguamento del sistema di sicurezza alle mutate normative introdotte dal D.Lgs. 81/08.
Per questo motivo il risultato della risk analysis è estremamente positivo e consente un giudizio prognostico favorevole alla serena prosecuzione dell'attività produttiva di SAN MARCO .
I documenti di valutazione dei rischi sono infatti adeguati alle prescrizioni del diritto e delle autorità, presentando le necessarie caratteristiche[3] di valutazione

adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.
5. In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti. Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla Commissione di cui all'articolo 6.
6. L'adozione del modello di organizzazione e di gestione di cui al presente articolo nelle imprese fino a 50 lavoratori rientra tra le attività finanziabili ai sensi dell'articolo 11.

[3] **Art. 28. Oggetto della valutazione dei rischi**
1. La valutazione di cui all'articolo 17, comma 1, lettera a), anche nella scelta delle attrezzature di lavoro e delle sostanze o dei preparati chimici impiegati, nonche' nella sistemazione dei luoghi di lavoro, deve riguardare tutti i rischi per la sicurezza e la salute dei lavoratori, ivi compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari, tra cui anche quelli collegati allo stress lavoro-correlato, secondo i contenuti dell'accordo europeo dell'8 ottobre 2004, e quelli riguardanti le lavoratrici in stato di gravidanza, secondo quanto previsto dal decreto legislativo 26 marzo 2001, n. 151, nonche' quelli connessi alle differenze di genere, all'eta', alla provenienza da altri Paesi.

dei rischi, di indicazione delle misure di prevenzione, di indicazione delle modalità di miglioramento del sistema nel tempo, di individuazione del responsabile del servizio di protezione e prevenzione, e delle mansioni che normalmente espongono i lavoratori ai rischi per la loro salute e sicurezza.
Quanto alla nomina dei rappresentanti dei lavoratori per la sicurezza, tale incombenza, è già stata assolta e risulta dal Documento di Valutazione dei Rischi già in vigore.
Le modalità di effettuazione della valutazione dei rischi rispettano anche le prescrizioni dell'art. 29 del D.Lgs. 81/08[4,]

2. Il documento di cui all'articolo 17, comma 1, lettera a), redatto a conclusione della valutazione, deve avere data certa e contenere:
a) una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa;
b) l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati, a seguito della valutazione di cui all'articolo 17, comma 1, lettera a);
c) il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
d) l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonche' dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
e) l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha partecipato alla valutazione del rischio; f) l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacita' professionale, specifica esperienza, adeguata formazione e addestramento.
3. Il contenuto del documento di cui al comma 2 deve altresi' rispettare le indicazioni previste dalle specifiche norme sulla valutazione dei rischi contenute nei successivi titoli del presente decreto.

[4] **Art. 29.Modalita' di effettuazione della valutazione dei rischi**
1. Il datore di lavoro effettua la valutazione ed elabora il documento di cui all'articolo 17, comma 1, lettera a), in collaborazione con il responsabile del servizio di prevenzione e protezione e il medico competente, nei casi di cui all'articolo 41.
2. Le attività di cui al comma 1 sono realizzate previa consultazione del rappresentante dei lavoratori per la sicurezza.
3. La valutazione e il documento di cui al comma 1 debbono essere rielaborati, nel rispetto delle modalita' di cui ai commi 1 e 2, in occasione di modifiche del processo produttivo o dell'organizzazione del lavoro significative ai fini della salute e della sicurezza dei lavoratori, o in relazione al grado di evoluzione della tecnica, della prevenzione e della protezione o a seguito di

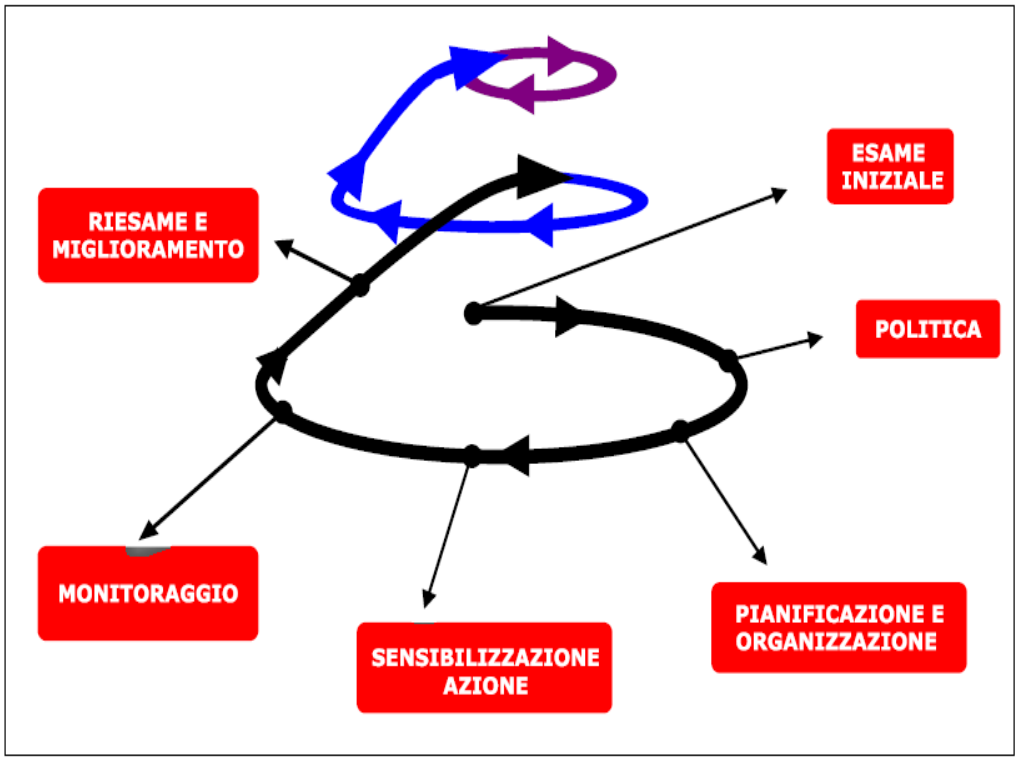
infortuni significativi o quando i risultati della sorveglianza sanitaria ne evidenzino la necessita'. A seguito di tale rielaborazione, le misure di prevenzione debbono essere aggiornate.
4. Il documento di cui all'articolo 17, comma 1, lettera a), e quello di cui all'articolo 26, comma 3, devono essere custoditi presso l'unita' produttiva alla quale si riferisce la valutazione dei rischi.
5. I datori di lavoro che occupano fino a 10 lavoratori effettuano la valutazione dei rischi di cui al presente articolo sulla base delle procedure standardizzate di cui all'articolo 6, comma 8, lettera f). Fino alla scadenza del diciottesimo mese successivo alla data di entrata in vigore del decreto interministeriale di cui all'articolo 6, comma 8, lettera f), e, comunque, non oltre il 30 giugno 2012, gli stessi datori di lavoro possono autocertificare l'effettuazione della valutazione dei rischi. Quanto previsto nel precedente periodo non si applica alle attività di cui all'articolo 31, comma 6, lettere a), b), c), d) nonché g).
6. I datori di lavoro che occupano fino a 50 lavoratori possono effettuare la valutazione dei rischi sulla base delle procedure standardizzate di cui all'articolo 6, comma 8, lettera f). Nelle more dell'elaborazione di tali procedure trovano applicazione le disposizioni di cui ai commi 1, 2, 3, e 4.
7. Le disposizioni di cui al comma 6 non si applicano alle attività svolte nelle seguenti aziende:
a) aziende di cui all'articolo 31, comma 6, lettere a), b), c), d), f) e g);
b) aziende in cui si svolgono attività che espongono i lavoratori a rischi chimici, biologici, da atmosfere esplosive, cancerogeni mutageni, connessi all'esposizione ad amianto;
c) aziende che rientrano nel campo di applicazione del titolo IV del presente decreto.

Come si può osservare infatti dalla matrice attività–reati, la valutazione ha tenuto conto dei seguenti parametri, in ossequio ai requisiti posti dall'art. 29 D.Lgs. 81/08:
- i documenti di valutazione dei rischi, sono stati redatti in collaborazione con il responsabile del servizio di prevenzione e protezione;
- il rappresentante dei lavoratori per la sicurezza è stato consultato per la redazione dei DVR;
- ogni DVR di SAN MARCO è un documento "aperto", suscettibile di rielaborazione ed integrazione in caso di significative modificazioni del processo produttivo o altre evoluzioni;
- i DVR sono custoditi presso l'unità produttiva.

Inoltre i Documenti di Valutazione dei Rischi redatti da SAN MARCO sono perfettamente adeguati alle linee guida UNI-INAIL come principi ispiratori della redazione del presente modello organizzativo:

ESAME INIZIALE: tale fase si è concretata nella indagine conoscitiva della realtà della società. e nel confronto dinamico fra le attività svolte e le fattispecie di rischio;
POLITICA: a seguito della valutazione dei rischi la società ha stabilito le priorità e le linee di attuazione delle contromisure;
PIANIFICAZIONE E ORGANIZZAZIONE: sono state individuate le innovazioni e modificazioni delle strutture e delle modalità operative necessarie per ovviare ai rischi segnalati;
SENSIBILIZZAZIONE: il personale è stato convocato per la formazione e l'aggiornamento sulle risultanze della valutazione dei rischi e sulle novità delle procedure;
MONITORAGGIO: l'Organismo di Vigilanza è incaricato di monitorare sulle materie affidate alla sua competenza, e di applicare gli interventi in caso di comportamenti difformi;
RIESAME E MIGLIORAMENTO: il Documento di Valutazione dei rischi di SAN MARCO è in continua evoluzione ad opera degli organismi incaricati, che suggeriscono ed attuano le modifiche ritenute necessarie.

La rappresentazione grafica della sequenza ciclica è la seguente:



Integrazione nel modello organizzativo dei sistemi di prevenzione per la salute e sicurezza in SAN MARCO

SAN MARCO ha perseguito un cammino di integrazione e coordinamento fra il Modello Organizzativo ai sensi del D.Lgs. 231/01 ed i sistemi dedicati alla prevenzione per la salute e sicurezza.
Infatti a seguito dell'analisi delle procedure esistenti del Sistema gestione sicurezza, è stato successivamente previsto un sistema di raccordo e trasmissione della documentazione relativa all'Organismo di Vigilanza,

realizzando in questa maniera una proficua integrazione fra i sistemi ed una accresciuta potenzialità di controllo e di prevenzione, nel pieno rispetto delle normative previste.

Il sistema di gestione della salute e sicurezza dei lavoratori in SAN MARCO rispetto alle prescrizioni dell'art. 30 D.lgs. 81/2008

Le prescrizioni dell'art. 30 D.lgs. 81/2008 impongono di dotarsi di un sistema organizzativo specificamente dedicato alla compliance su alcuni temi ritenuti di primaria importanza per garantire un corretto approccio al tema della salute e sicurezza dei lavoratori.
SAN MARCO ha da tempo adottato tutte le misure necessarie a garantire tale tutela, e pertanto non si è ritenuto necessario intervenire sugli aspetti tecnici della prevenzione operativa.
L'intervento si è quindi focalizzato sugli aspetti organizzativi della prevenzione, operando in particolar modo sulla costituzione dell'Organismo di Vigilanza 231, e sulle sue prerogative di controllo della corretta sequenza degli adempimenti tecnici svolti dalle autorità a ciò deputate.
Si struttura quindi un nuovo soggetto che affianca e formalizza l'attività delle altre strutture.
Il nucleo dell'intervento organizzativo si attesta pertanto sulla predisposizione delle misure di raccordo fra quelle strutture e l'Organismo di Vigilanza. Inoltre risulta necessario introdurre, anche alla luce delle nuove normative analizzate, delle procedure indispensabili per guidare l'operatività dell'Organismo di Vigilanza nominato ai sensi dell'art. 6 del D.lgs. 231/2001, che svolge un ruolo di estrema importanza nella supervisione degli adempimenti imposti dalle suddette normative. Questo al fine di rendere il sistema maggiormente efficace ed efficiente.
Il modello organizzativo di SAN MARCO ha quindi introdotto un meccanismo di coordinamento fra questo organismo e le autorità deputate, in azienda, al controllo del sistema di sicurezza del lavoro, in linea con i dettami dell'art. 30 del D.Lgs. 81/08, che prevede quindi una opportuna attività di reporting verso l'Organismo di Vigilanza come di seguito illustrato.

Le nuove procedure organizzative di SAN MARCO relative alla salute e sicurezza dei lavoratori

Per quanto riguarda le procedure della Sicurezza, viene aggiunta la seguente modalità operativa.

PROCEDURA GENERALIZZATA DI TRASMISSIONE DOCUMENTAZIONE ALL'ORGANISMO DI VIGILANZA

L'RSPP responsabile, con l'ausilio dei consulenti appositamente nominati, dovrà curare la predisposizione da parte dei documenti relativi alla organizzazione e gestione delle emergenze e del primo soccorso; dovrà verbalizzare le consultazioni dei rappresentanti dei lavoratori per la sicurezza, ed infine dovrà trasmettere con le modalità di seguito indicate i risultati di tali adempimenti all'O.d.V. Dovrà inoltre attestare l'acquisizione di documentazione e certificazioni obbligatorie di legge, trasmettendo con cadenza annuale un report all'O.d.V. sull'attuazione delle informazioni comunicate dall'ufficio tecnico interno.

Il sistema dei controlli

Fermo restando il potere discrezionale dell'O.d.V. di attivarsi con specifici controlli, anche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello) e ferme restando le specifiche

attribuzioni di cui al precedente paragrafo, l'O.d.V. effettua periodicamente, anche coadiuvato da soggetti terzi, controlli a campione sulle attività sociali potenzialmente a rischio di commissione di reati societari, al fine di verificare che la gestione concreta di tali attività avvenga in maniera conforme alle regole e coerente con i principi dettati dal presente Modello (esistenza e adeguatezza della relativa procura, limiti di spesa, effettuato reporting verso gli organi deputati, ecc.).
In ragione dell'attività di vigilanza attribuita all'O.d.V. nel presente Modello, a tale organismo viene garantito, in generale, libero accesso a tutta la documentazione aziendale che lo stesso ritiene rilevante al fine del monitoraggio dei Processi Sensibili individuati nella presente Parte Speciale (vedi Parte Generale).

I DELITTI CONTRO LA PERSONALITA' INDIVIDUALE

Considerazioni Generali

L'art. 5 della Legge 11 agosto 2003, n. 228 ha introdotto, nel corpo del D. Lgs. 231/2001 (di seguito, 'Decreto'), l'art. 25-quinquies, il quale prevede la responsabilità degli enti per i delitti contro la personalità individuale, commessi dai propri soggetti apicali o subordinati nell'interesse e/o vantaggio della società stessa.
Art. 25-quinquies.
Delitti contro la personalità individuale (1)

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

a) per i delitti di cui agli articoli 600, 601, 602 e 603-bis, la sanzione pecuniaria da quattrocento a mille quote; (3)

b) per i delitti di cui agli articoli 600-bis, primo comma, 600-ter, primo e secondo comma, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, e 600-quinquies, la sanzione pecuniaria da trecento a ottocento quote; (2)

c) per i delitti di cui agli articoli 600-bis, secondo comma, 600-ter, terzo e quarto comma, e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, nonché per il delitto di cui all'articolo 609-undecies la sanzione pecuniaria da duecento a settecento quote. (2)

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

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

(1) Articolo aggiunto dalla L. 11 agosto 2003, n. 228.
(2) Lettera così modificata dall'art. 10, comma 1, lett. b), L. 6 febbraio 2006, n. 38 e, successivamente, dall'art. 3, comma 1, D.Lgs. 4 marzo 2014, n. 39.
(3) Lettera così modificata dall’art. 6, comma 1, L. 29 ottobre 2016, n. 199, a decorrere dal 4 novembre 2016, ai sensi di quanto disposto dall’art. 12, comma 1, della medesima legge n. 199/2016.

Le fattispecie di reato indicate

Art. 600 c.p. - Riduzione o mantenimento in schiavitù o in servitù.
«Chiunque esercita su una persona poteri corrispondenti a quelli del diritto di proprietà ovvero chiunque riduce o mantiene una persona in uno stato di

soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento, è punito con la reclusione da otto a venti anni.
La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta è attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona.
La pena è aumentata da un terzo alla metà se i fatti di cui al primo comma sono commessi in danno di minore degli anni diciotto o sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi».

La norma descrive due ipotesi delittuose: rispettivamente la «riduzione o mantenimento in schiavitù» e «riduzione o mantenimento in servitù».
La prima riconduce alla nozione di “schiavitù” “all’esercizio su una persona poteri corrispondenti a quelli del diritto di proprietà”. Quindi sono compresi sia le tipiche facoltà inerente al diritto di proprietà, cioè godere e disporre, sia l’esercizio di diritti reali minori.
Invece la seconda figura prescinde dal richiamo al diritto domenicale e si distingue due momenti: lo sfruttamento coattivo di una persona e la condizione di assoggettamento dall’altro. La sinergia tra queste due condizioni permette di individuare il reato de quo quando la persona diventa una “cosa” poiché la sua vita è interamente determinata a sistematicamente finalizzata per la realizzazione di utilità godute da soggetti terzi. Sul piano strutturale siamo di fronte ad un reato complesso: lo sfruttamento è un effetto della costrizione che deve essere l’espressione di una situazione di soggezione continua. Per “costringimento” si deve intendere assoggettamento ad attività contra voluntatem e per “sfruttamento” non è esaustiva la sua connotazione esclusivamente economica. Due sono, quindi, i momenti della fattispecie: lo sfruttamento coattivo di una persona da un lato, e la condizione di assoggettamento del soggetto sfruttato dall’altro. Lo sfruttamento deve avere a oggetto le prestazioni della vittima: questa utilità dovrà essere effettivamente percepita.
Con riferimento ai reati connessi alla schiavitù, va ricordato che tali ipotesi di reato si estendono non solo al soggetto che direttamente realizza la fattispecie

illecita, ma anche a chi consapevolmente agevola anche solo finanziariamente la medesima condotta.
Ex D.lgs. 231/2001, la condotta rilevante in questi casi è costituita dal procacciamento illegale della forza lavoro attraverso il traffico di migranti e la tratta degli schiavi.

Art. 600-bis c.p. - Prostituzione minorile.
«E' punito con la reclusione da sei a dodici anni e con la multa da euro 15.000 a euro 150.000 chiunque:
1) recluta o induce alla prostituzione una persona di età inferiore agli anni diciotto;
2) favorisce, sfrutta, gestisce, organizza o controlla la prostituzione di una persona di età inferiore agli anni diciotto, ovvero altrimenti ne trae profitto.
Salvo che il fatto costituisca più grave reato, chiunque compie atti sessuali con un minore di età compresa tra i quattordici e i diciotto anni, in cambio di un corrispettivo in denaro o altra utilità, anche solo promessi, è punito con la reclusione da uno a sei anni e con la multa da euro 1.500 a euro 6.000».

Il reato di prostituzione minorile ex art. 600-bis, comma 2, c.p. si consuma al momento del compimento dell'atto sessuale in cambio di un corrispettivo. Tuttavia, prima di allora, si configura il delitto tentato, in tutte le ipotesi in cui l'agente non riesce a portare a termine il delitto programmato per cause indipendenti dalla propria volontà, ma gli atti parzialmente realizzati sono comunque tali da esteriorizzare la sua intenzione criminosa, che non si ferma allo stadio di semplice proposito, ma è manifestata all'esterno proprio con il compimento di atti idonei a commettere il delitto.

Art. 600-ter c.p. - Pornografia minorile.
«E' punito con la reclusione da sei a dodici anni e con la multa da euro 24.000 a euro 240.000 chiunque:
1) utilizzando minori di anni diciotto, realizza esibizioni o spettacoli pornografici ovvero produce materiale pornografico;

2) recluta o induce minori di anni diciotto a partecipare a esibizioni o spettacoli pornografici ovvero dai suddetti spettacoli trae altrimenti profitto.
Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma.
Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o diffonde notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da euro 2.582 a euro 51.645.
Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, offre o cede ad altri, anche a titolo gratuito, il materiale pornografico di cui al primo comma, è punito con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.1642.
Nei casi previsti dal terzo e dal quarto comma la pena è aumentata in misura non eccedente i due terzi ove il materiale sia di ingente quantità".
"Salvo che il fatto costituisca più grave reato, chiunque assiste a esibizioni o spettacoli pornografici in cui siano coinvolti minori di anni diciotto è punito con la reclusione fino a tre anni e con la multa da euro 1.500 a euro 6.000.
Ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali».

Affinché vi sia divulgazione o distribuzione occorre, che l'agente inserisca le foto pornografiche minorili in un sito accessibile a tutti, al di fuori di un dialogo "privilegiato" come può essere una chat-line, o le invii ad un gruppo o lista di discussione, da cui chiunque le possa scaricare, o le invii bensì ad indirizzi di persone determinate ma in successione, realizzando cioè una serie di conversazioni private (e, quindi, di cessioni) con diverse persone.
Di conseguenza l'uso dello strumento Internet non è sufficiente da sé a integrare, sempre e comunque, una comunicazione ad un numero indeterminato di persone, essendo, al contrario, necessario analizzare di volta in volta il singolo caso concreto per poter rilevare ed accertare il tipo di comunicazione, "aperta o

chiusa", che il soggetto interessato ha posto in essere. In definitiva è da escludere che la trasmissione diretta tra due utenti, i quali devono essere necessariamente d'accordo sulla trasmissione del materiale, configuri senz'altro una divulgazione o distribuzione ai sensi del terzo comma della norma citata, più coerente appare la configurazione del quarto comma dell'art. 600-ter c.p.

Art. 600-quater c.p. - Detenzione di materiale pornografico.
«Chiunque, al di fuori delle ipotesi previste nell'articolo 600-ter, consapevolmente si procura o dispone di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori degli anni diciotto è punito con la reclusione fino a tre anni o con la multa non inferiore a euro 1.549".
La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia d'ingente quantità».

A differenza dell'art. 600-ter c.p., che è configurabile quando la condotta dell'agente abbia una consistenza tale da implicare concreto pericolo di diffusione del materiale pornografico prodotto, per la configurabilità del reato di cui all'art. 600-quater c.p. non è necessaria la sussistenza di tale pericolo, essendo sufficiente la consapevole detenzione del materiale.
Può definirsi di "ingente quantità" un numero molto grande, rilevante o consistente d'immagini pedopornografiche il cui possesso contribuisca concretamente ad alimentarne l'illecito mercato.

Non c'è concorso tra il reato di detenzione di materiale pedopornografico con quello di cessione dello stesso, in quanto la prima fattispecie è da ritenersi assorbita da quest'ultima.

Articolo 600-quater 1 c.p. – Pornografia virtuale.

«Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo.

Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali».

Il bene giuridico tutelato è costituito esclusivamente dall'integrità fisica, psicologica, morale e sociale del minore eventualmente rappresentato nelle immagini, sicché vanno esclusi dalla previsione normativa i disegni pornografici e dunque anche cartoni animati che rappresentano bambini e adolescenti di fantasia. La detenzione di tali immagini sarebbe al più sussumibile nella fattispecie di cui all'art. 528 c.p. (Pubblicazioni e spettacoli osceni) ove però sussista lo scopo ulteriore di commercio, distribuzione o esposizione al pubblico. Vanno così distinte tre categorie d'immagini virtuali:
1) immagini e video bidimensionali o tridimensionali realizzate come disegni anche con la tecnica del "cartone animato", immediatamente indicative di creazione di fantasia; 2) immagini tridimensionali rappresentanti soggetti minorenni non confondibili con persone reali, ancorché realizzato nel rispetto delle proporzioni, il prodotto finale è costituito dalla creazione grafica a computer di figure all'evidenza del tutto simili non a persone reali ma a "manichini" impegnati in atti sessuali;
3) immagini tridimensionali, realizzate con elevata qualità grafica che rappresentano figure umane plastiche e proporzionate di adulti e minori coinvolti in atti sessuali dove alla sommità del corpo del minorenne è stata apposta l'immagine bidimensionale ritraente un bambino realmente esistente.
Le immagini di cui alle categorie 1) e 2) sono disegni che riproducono soggetti "virtuali" perché costruiti con il computer ma non suscettibili di essere confusi, anche per qualità grafica, con persone reali e dunque né rappresentative né evocative di situazioni reali.

Art. 600-quinquies c.p. - Iniziative turistiche volte allo sfruttamento della prostituzione minorile.
«Chiunque organizza o propaganda viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori o comunque comprendenti tale attività è punito con la reclusione da sei a dodici anni e con la multa da euro 15.493 e euro 154.937».

La ratio della fattispecie di cui all'art. 600-quinquies c.p. è di anticipare la tutela penale alla soglia delle attività prodromiche e collaterali all'induzione, al favoreggiamento, allo sfruttamento della prostituzione dei minori. Il delitto in questione rientra pertanto nella categoria dei reati di mera condotta e di pericolo astratto, perché tende a prevenire - con la previsione della punizione di talune condotte in via decisamente anticipata - tutto ciò che agevola l'incontro tra domanda e offerta.
Tuttavia, al fine punire chi «organizza (o pubblicizza) iniziative turistiche aventi lo scopo, anche se non unico, di favorire gli interessati a entrare in contatto con minori a fini sessuali», è comunque necessario che sia realizzata una specifica condotta di tipo organizzativo, consistente nella programmazione dei viaggi illeciti, con quanto di utile al buon esito della trasferta (vettore, supporti logistici etc.), includendo anche idonei servizi inerenti la possibilità di entrare in contatto con l'ambiente della prostituzione minorile. Nella prestazione di tali servizi, peraltro, possono rientrare anche mere condotte di facilitazione, come la fornitura d'indirizzi e di informazioni essenziali su luoghi e persone.
Ai fini della condotta organizzativa rilevante ai sensi dell'art. 600-quinquies c.p. non si richiede che l'agente sia un operatore turistico.

Art. 609-undecies c.p. - Adescamento di minorenni.

«Chiunque, allo scopo di commettere i reati di cui agli articoli 600, 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-quater, 609-quinquies e 609-octies, adesca un minore di anni sedici, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a tre anni. Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce

posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione».

Trattasi di una fattispecie residuale rispetto a ipotesi di reato più gravi. Persona offesa dal reato è il minore di anni sedici. La condotta di adescamento, così definita, deve, inoltre, essere finalizzata alla commissione dei reati di cui agli artt. 600 c.p. (riduzione o mantenimento in schiavitù o servitù), 600-bis c.p. (prostituzione minorile), 600-ter c.p. (pornografia minorile) e 600-quater c.p. (detenzione di materiale pornografico, anche se si tratti del materiale pornografico "virtuale" di cui all'art. 600-quater1 c.p.), ovvero a quelli di cui agli artt. 600-quiquies (iniziative turistiche volte alla sfruttamento della prostituzione minorile), 609-bis (violenza sessuale), 609-quater (atti sessuali con minorenne), 609-quinquies (corruzione di minorenne), 609-octies (violenza sessuale di gruppo). In altri termini la condotta di adescamento si caratterizza per il dolo specifico, ovverosia l'intento, di commettere uno dei citati reati. Trattandosi, come detto, di fattispecie residuale l'eventuale commissione di tali reati esclude che si possa configurare l'ipotesi di cui al 609-undecies c.p.
Si tratta, secondo la dottrina, di un reato di pericolo concreto, ove la soglia della punibilità è arretrata al semplice pericolo di lesione del bene giuridico tutelato, ovverosia la libertà di autodeterminazione dell'individuo (minore degli anni sedici), nella forma della libertà sessuale. Si ritiene, in ogni caso, che, pur essendo sufficiente a integrare il reato un singolo atto di adescamento, è indispensabile che questo si realizzi attraverso atteggiamenti idonei a renderlo in concreto capace di carpire la fiducia della vittima, convogliandola verso i fini criminosi che hanno animato le intenzioni del reo.

Art. 601 c.p. - Tratta di persone.
«Chiunque commette tratta di persona che si trova nelle condizioni di cui all'articolo 600 ovvero, al fine di commettere i delitti di cui al medesimo articolo, la induce mediante inganno o la costringe mediante violenza, minaccia, abuso di autorità o di una situazione d'inferiorità fisica o psichica o di una situazione di necessità, o mediante promessa o dazione di somme di denaro o di altri vantaggi alla persona che su di essa ha autorità, a fare ingresso o a soggiornare o a uscire

dal territorio dello Stato o a trasferirsi al suo interno, è punito con la reclusione da otto a venti anni.
La pena è aumentata da un terzo alla metà se i delitti di cui al presente articolo sono commessi in danno di minore degli anni diciotto o sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi».

Due sono le condotte previste dall'art. 601, comma 1, c.p. La prima comprende "commettere la tratta"; la seconda a "indurre o costringere qualcuno" mediante inganno o mediante violenza, minaccia, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante promessa o dazione di somme di denaro o di altri vantaggi alla persona che su di essa ha autorità, a fare ingresso o a soggiornare o a uscire dal territorio dello Stato o a trasferirsi al suo interno. In realtà si tratta di un unico tipo di condotta che si diversifica solo in relazione alle caratteristiche della vittima. Infatti questa deve essere o meno già ridotta in stato di schiavitù.
La fattispecie richiede anche la finalità del primo comma dell'art. 600 c.p. cioè ridurre in schiavitù o in servitù. Quindi si consuma anticipatamente rispetto all'effettiva riduzione in schiavitù o servitù.
Caratteristica di questa norma è la libertà della vittima: è uno di quei reati che si definisce di "cooperazione artificiosa" perché si consuma quando la vittima, anche se indotta o coartata nella sua volontà, fa ingresso o vi soggiorni, esca o si trasferisca all'interno del territorio dello Stato.

Art. 602 c.p. - Acquisto e alienazione di schiavi.
«Chiunque, fuori dei casi indicati nell'articolo 601, acquista o aliena o cede una persona che si trova in una delle condizioni di cui all'articolo 600 è punito con la reclusione da otto a venti anni.
La pena è aumentata da un terzo alla metà se la persona offesa è minore degli anni diciotto ovvero se i fatti di cui al primo comma sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi».

Per configurare autonomamente la fattispecie è necessario l'imprenditorialità o una dimensione organizzativa ampia e stabile. Nel fatto tipico rimangono solo le condotte di acquisto, alienazione, cessione di esseri umani.
Si sostiene che con questa fattispecie siano esauriti tutti possibili i casi di trasmissione per atto di volontà del potere sullo schiavo sia a titolo oneroso che gratuito.

Art. 603-Bis c.p. - Intermediazione illecita e sfruttamento del lavoro.
«Salvo che il fatto costituisca più grave reato, è punito con la reclusione da uno a sei anni e con la multa da 500 a 1.000 euro per ciascun lavoratore reclutato, chiunque:
1) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;
2) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.
Se i fatti sono commessi mediante violenza o minaccia, si applica la pena della reclusione da cinque a otto anni e la multa da 1.000 a 2.000 euro per ciascun lavoratore reclutato.
Ai fini del presente articolo, costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni:
1) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;
2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.
Costituiscono aggravante specifica e comportano l'aumento della pena da un terzo alla metà:
1) il fatto che il numero di lavoratori reclutati sia superiore a tre;
2) il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa;

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

La Legge 199/2016 ha operato un intervento volto a rafforzare il contrasto al cosiddetto "caporalato", modificando il testo dell'art. 603-bis c.p. concernente il reato di «Intermediazione illecita e sfruttamento del lavoro» introdotto per la prima volta con il D.L. 138/2011, convertito con modificazioni dalla L. 148/2011.

Rispetto al testo previgente, volto a punire la condotta di chi svolgesse «un'attività organizzata di intermediazione, reclutando manodopera o organizzandone l'attività lavorativa caratterizzata da sfruttamento, mediante violenza, minaccia o intimidazione, approfittando dello stato di bisogno o di necessità dei lavoratori», la nuova fattispecie risulta sicuramente ampliata.

Il reato in esame, oggi, risulta slegato dal requisito dello svolgimento di «un'attività organizzata di intermediazione», andando a colpire non solo chi «recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento…», ma altresì chiunque «utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno».

A ciò deve aggiungersi che integra il reato de quo, rispetto alla fattispecie previgente, anche la condotta non caratterizzata da violenza, minaccia o intimidazione, posto che la violenza e la minaccia sono divenute oggi circostanze aggravanti e non più elementi costitutivi del reato.

Anche gli "indici di sfruttamento" enunciati dall'art. 603-bis c.p. assumono una connotazione più ampia, essendo oggi alcuni di essi parametrati, ad esempio, non più a condotte sistematiche di sotto retribuzione e violazione delle norme su orari, riposi, aspettativa e ferie, bensì a siffatte condotte anche solo «reiterate».

Di particolare rilievo è anche l'indice di sfruttamento relativo alla «sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro» che oggi, a differenza di prima, rileva anche laddove non sia tale da esporre il lavoratore a pericolo per la salute, la sicurezza o l'incolumità personale.

Il «grave pericolo», infatti, rileva ora solo quale circostanza aggravante ai sensi del comma 4 punto 3).

Inoltre si evidenzia che nel contesto di tale indice non rileva neppure la reiterazione della condotta.

La punibilità dell'ente è dunque collegata al compimento di un reato non più limitato a chi svolge attività organizzata d'intermediazione, né legato a violenza e minaccia come elementi costitutivi; reato connotato inoltre da «uno sfruttamento» la cui presenza a dedotta dalla semplice reiterazione di condotte di retribuzione palesemente difforme dai contratti collettivi nazionali o territoriali, dalla violazione delle norme su orario, riposo, aspettativa e ferie o dalla mera sussistenza di violazione delle norme antinfortunistiche, anche non tali da esporre a pericolo il lavoratore.
A contemperamento di una siffatta estensione nella possibile applicazione della norma, si deve tuttavia considerare la natura dolosa del reato in esame, con la conseguenza che le condotte costituenti "indice di sfruttamento" rileveranno solo ove dolosamente preordinate a sottoporre «i lavoratori a condizioni di sfruttamento» con consapevolezza e volontà di approfittare «del loro stato di bisogno».
Le sanzioni per l'ente sono le stesse gravissime sanzioni disposte per i diversi reati di «Riduzione o mantenimento in schiavitù o in servitù» (art. 600 c.p.), «Tratta di persone» (art. 601 c.p.) e «Acquisto e alienazione di schiavi» (art. 602 c.p.):
– sanzione pecuniaria da 400 a 1000 quote;
– sanzioni interdittive di cui all'art. 9, co. 2 D.Lgs. 231/01, senza esclusioni, per una durata non inferiore a un anno;
– interdizione definitiva dall'attività, se l'ente o una sua unità organizzativa sono stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione del reato.

AREE "A RISCHIO REATO" E PRINCIPI DI CONTROLLO

Preliminarmente, si deve segnalare come la commissione dei sopramenzionati reati risulti di difficile attuazione con riferimento alla realtà societaria considerata. In ogni caso, per completezza, in occasione dell'implementazione dell'attività di risk mapping, sono state individuate, per la tipologia dei reati in questione, le seguenti possibili aree di rischio che, all'interno della struttura di SAN MARCO , possono definirsi potenziali:

1. Acquisti di beni e servizi;
2. Selezione e Assunzione del Personale/Talent Acquisition;
3. Amministrazione del Personale;
4. Gestione sistemi informativi/Information Technology;

Fermo restando i controlli previsti dalle procedure aziendali e meglio dettagliati nelle diverse Parti Speciali, le regole definite nel Modello di organizzazione, gestione e controllo, nell'espletamento delle rispettive attività/funzioni, tutti i destinatari devono seguire i seguenti principi di controllo:

 la selezione delle controparti destinate a fornire i servizi, siano essi Partner o Fornitori, deve essere svolta con particolare attenzione e in base ad apposita procedura interna;

 in caso di assunzione diretta di personale da parte di SAN MARCO , deve essere verificato il rispetto delle norme giuslavoristiche e degli accordi sindacali per l'assunzione e il rapporto di lavoro in generale. nonché il rispetto delle regole di correttezza e di buon comportamento nell'ambiente di lavoro;

 tutti gli esponenti aziendali devono rispettare le specifiche previsioni contenute nel Modello Organizzativo volte a contrastare comportamenti configurabili i reati della presente Parte Speciale;

 devono essere utilizzati strumenti informatici costantemente aggiornati ed elaborati da reputate imprese del settore che impediscano l'accesso e/o ricezione di materiale relativo alla pornografia minorile (strumenti di "content filtering");

 nel rispetto delle normative vigenti, l'Azienda svolge periodici controlli volti ad impedire l'abuso dei sistemi informativi aziendali o la commissione di reati attraverso il loro utilizzo;

 devono essere effettuati richiami netti e inequivocabili volti al corretto uso degli strumenti informatici in possesso dei dipendenti;

 deve essere svolta una attenta valutazione di possibili partnership commerciali con società operanti in settori quali la comunicazione telematica di materiale relativo alla pornografia minorile e il turismo nelle aree geografiche richiamate al punto precedente;

 assunzione dello specifico impegno da parte dei propri partner consistente nel rispetto de gli obblighi di legge in tema di: tutela del lavoro minorile e delle donne; condizioni igienico-sanitarie e di sicurezza; diritti sindacali o di associazione e rappresentanza. Ai fini della verifica del rispetto di tale impegno, l'ente può prevedere visite ispettive presso i propri fornitori ovvero richiedere loro ogni documentazione utile;

 nei contratti con i collaboratori esterni, deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto nonché dei principi contenuti nel Modello.

PRINCIPI GENERALI DI COMPORTAMENTO

Le risorse aziendali coinvolte nelle aree “a rischio reato” sono tenute, nell’ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello.
È fatto assoluto divieto di:
- tenere, promuovere, 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 considerate nelle presente Parte Speciale (art. 25-quinquies del Decreto);
- tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- utilizzare anche occasionalmente la Società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei reati di cui alla presente Parte Speciale.
Chiunque rilevi una gestione anomala del personale o dei soggetti in qualunque modo in forza a SAN MARCO , è tenuto ad informare immediatamente l’Organismo di Vigilanza.

Parte Speciale 5: REATI AMBIENTALI

Il D.Lgs 231/2001 e i reati ambientali

Le origini comunitarie della tutela penale dell'ambiente

L'Unione europea ha dato da sempre una spinta determinante al processo di costruzione del diritto penale dell'ambiente. La consapevolezza che l'inquinamento costituisce un fenomeno globale, infatti, ha imposto l'adozione di provvedimenti di carattere sovranazionale.
Già nel 1998 il Consiglio d'Europa, decise di adottare una Convenzione per la tutela dell'ambiente attraverso il diritto penale (mai entrata in vigore per il ridotto numero di ratifiche), che rappresenta tuttavia il primo strumento internazionale che ha previsto la criminalizzazione da parte degli Stati membri dell'UE di una serie di condotte produttive di danno o pericolo per l'ambiente. Invero, scopo ultimo della Convenzione era imporre agli Stati l'introduzione nei codici penali di fattispecie di reato di pericolo, anticipando, così, la soglia di tutela del bene, nonché la predisposizione di una responsabilità a titolo di colpa, quanto meno in riferimento ai casi di colpa grave.
Nel 2001 la Commissione europea, visto il tentativo mal riuscito nel 1998, predispose un testo per una direttiva in materia, mentre il Consiglio dei Ministri dell'Unione europea il 27 gennaio 2003 assunse la decisione quadro 2003/80/GAI, nota per esser stata oggetto di ricorso da parte della Commissione europea per un conflitto di competenza istituzionale, risolto dalla sentenza della Corte di Giustizia del 13 settembre 2005, Causa C-176/03, nella quale i giudici europei confermarono che una decisione in materia di protezione dell'ambiente mediante il diritto penale avrebbe dovuto avere come fondamento giuridico il trattato CE e non il trattato sull'Unione europea (trattato UE).
Va ricordato inoltre che la Commissione Europea ha emanato la Direttiva 2004/35/CE con la quale ha inteso fornire un contributo determinante nella costruzione di un sistema normativo condiviso in tema di responsabilità per danni all'ambiente, pur senza introdurre fattispecie penali, ma prescrivendo obblighi e responsabilità a carico degli operatori economici in caso di causazione di danni.
Ma l'atto decisamente più significativo è rappresentato dalla Direttiva 2008/99/CE sulla tutela penale dell'ambiente del 19 novembre 2008.

Il recepimento delle Direttive Europee

Il 7 luglio 2011 è stato approvato dal Consiglio dei Ministri il D.Lgs. 121/2011 che ha recepito la Direttiva 2008/99 CE, relativa alla tutela penale dell'ambiente, e la 2009/123 CE che modifica la Direttiva 2005/35/CE (relativa all'inquinamento provocato dalle navi). Tale Decreto, entrato in vigore il 16 agosto 2011, modifica il D.Lgs. 231/2001 estendendo agli Enti la responsabilità amministrativa anche per i reati ambientali.
Dal 2001, data di entrata in vigore del D.Lgs. 231, diversi sono stati i decreti legislativi introdotti che, nel corso degli anni hanno incrementato le fattispecie dei reati presupposto previsti dalla normativa che disciplina la Responsabilità Amministrativa degli Enti. Nel 2007 sono stati introdotti i Reati colposi in violazione di adempimenti in materia di Sicurezza sul lavoro; nel 2008 il riciclaggio/ricettazione ed il delitti informatici; nel 2009 i delitti contro l'industria ed il commercio, la violazione dei diritti d'autore e quelli di criminalità organizzata ed infine nel 2011 i reati ambientali.

Coordinamento delle politiche aziendali

A seguito dell'introduzione dei Reati ambientali tra le fattispecie dei reati previsti nel D.Lgs. 231/2001 nasce l'esigenza di creare un chiaro e strutturato collegamento e coordinamento delle politiche e dei sistemi aziendali per la gestione delle tematiche ambientali con il Modello Organizzativo.
A differenza di quanto previsto per il Reati in materia di salute e sicurezza, l'art. 25 undecies del D.Lgs 231/2001 non prevede al momento una diretta condizione esimente nel caso in cui l'Ente abbia adottato un sistema di gestione ambientale certificato. Si rende quindi indispensabile definire e documentare in modo esaustivo ed efficace le modalità di raccordo del sistema di procedure e presidi in materia ambientale adottato dalla società ed il Modello Organizzativo.
L’adozione di un sistema di Gestione Ambientale ben strutturato rappresenta indubbiamente un elemento rafforzativo di notevole rilievo per la sostenibilità del modello 231 alla luce dei nuovi dettami normativi ma non esonera la società dalla dimostrazione di aver stabilito gli “specifici protocolli” richiesti dalla norma, volti ad evitare la commissione di un illecito ambientale.
L’esistenza di una serie di procedure con compiti, ruoli, risorse, tempi e responsabilità definite e codificate sulla base delle best practice e dei Modelli Certificati, costituisce un presupposto essenziale per la corretta interpretazione e attuazione delle politiche ambientali all’interno dell’azienda. Inoltre, tale sistema

consente di migliorare l'identificazione e la valutazione degli aspetti ambientali, garantire il rispetto delle prescrizioni legali, rendere più efficiente la sorveglianza, la misurazione e la risposta ad eventuali emergenze ambientali.

L' introduzione dei nuovi reati all'interno del codice penale

Il D.Lgs. 121/2011 introduce nel codice penale e nel novero dei reati di cui al D.Lgs. 231/2001 due nuove fattispecie di reato per sanzionare la condotta di chi uccide, distrugge, preleva o possiede, fuori dai casi consentiti, esemplari di specie animali o vegetali selvatiche protette e di chi distrugge, o comunque deteriora in modo significativo, un habitat all'interno di un sito protetto. Nello specifico, sono stati introdotti gli articoli:

- **727 bis c.p.**: punisce diverse tipologie di condotte illecite nei confronti di specie animali e vegetali selvatiche protette ovvero:
a) la condotta di chi , fuori dai casi consentiti, uccide, cattura o detiene esemplari appartenenti ad una specie selvatica protetta, sanzionandole in via alternativa con l'arresto da 1 a 6 mesi o con l'ammenda fino a 4.000 euro (comma 1);
b) la condotta di chi, fuori dai casi consentiti, distrugge,preleva o detiene esemplari appartenenti ad una specie vegetale selvatica protetta, prevedendo un'ammenda fino a 4.000 euro (comma 2);

1. **733 bis c.p.**: punisce la distruzione o deterioramento di habitat all'interno di un sito protetto. L'illecito contravvenzionale punisce con la pena dell'arresto fino a 18 mesi e con l'ammenda non inferiore ad euro 3.000 chiunque, fuori dai casi consentiti, distrugge un habitat all'interno di un sito protetto o comunque lo deteriora compromettendone lo stato di conservazione. Ai fini dell'applicazione dell'art. 733 bis c.p. per "habitat all'interno di un sito protetto" si intende qualsiasi habitat di specie per le quali una zona sia classificata come zona a tutela speciale a norma dell'art. 4 paragrafi 1 o 2, della Direttiva 79/409/CE, o qualsiasi habitat naturale o un habitat di specie per cui un sito sia designato come zona speciale di conservazione a norma dell'art.4, paragrafo 4, della Direttiva 92/437 CE".

Il nuovo art. 25 undecies del D.Lgs 231/2001

Il D.Lgs 121/2011 ha introdotto nel D.Lgs. 231/2001 l'art. 25 undecies il quale prevede un nuovo catalogo di reati presupposto della Responsabilità degli Enti. Nello specifico l'art. 25 undecies identifica come reati presupposto della Responsabilità Amministrativa degli Enti:

1. Reati previsti dal codice penale

2. Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.)
3. Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.)

2. Reati previsti dal Codice dell'Ambiente di cui al D.Lgs. 3 aprile 2006, n. 152

4. Inquinamento idrico (art. 137):

   - scarico non autorizzato (autorizzazione assente, sospesa o revocata) di acque reflue industriali contenenti sostanze pericolose (co. 1 e 2);

   - scarico di acque reflue industriali contenenti sostanze pericolose in violazione delle prescrizioni imposte con l'autorizzazione o da autorità competenti (co. 3);

   - scarico di acque reflue industriali contenenti sostanze pericolose in violazione dei limiti tabellari o dei limiti più restrittivi fissati da Regioni o Province autonome o dall'Autorità competente (co. 5, primo e secondo periodo);

- violazione dei divieti di scarico sul suolo, nelle acque sotterranee e nel sottosuolo (co. 11);

- scarico in mare da parte di navi o aeromobili di sostanze o materiali di cui è vietato lo sversamento, salvo in quantità minime e autorizzato da autorità competente (co. 13);

5. Gestione di rifiuti non autorizzata (art. 256):

- raccolta, trasporto, recupero, smaltimento, commercio e intermediazione di rifiuti, non pericolosi e pericolosi, in mancanza della prescritta autorizzazione, iscrizione o comunicazione (art. 256, co. 1, lett. a) e b);

- realizzazione o gestione di una discarica non autorizzata (art. 256, co. 3, primo periodo);

- realizzazione o gestione di discarica non autorizzata destinata, anche in parte, allo smaltimento di rifiuti pericolosi (art. 256, co. 3, secondo periodo);

- attività non consentite di miscelazione di rifiuti (art. 256, co. 5);

- deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi (art. 256, co. 6);

6. Siti contaminati (art. 257):

- inquinamento del suolo, del sottosuolo, delle acque superficiali e delle acque sotterranee con il superamento delle concentrazioni soglia di rischio (sempre che non si provveda a bonifica, in conformità al progetto approvato dall'autorità competente) e omissione della relativa comunicazione agli enti competenti (co. 1 e 2). La condotta di inquinamento di cui al co. 2 è aggravata dall'utilizzo di sostanze pericolose.

7. Falsificazioni e utilizzo di certificati di analisi di rifiuti falsi (artt. 258 e 260-bis)

- predisposizione di un certificato di analisi dei rifiuti falso (per quanto riguarda le informazioni relative a natura, composizione e caratteristiche chimico-fisiche dei rifiuti) e uso di un certificato falso durante il trasporto (art. 258, co. 4, secondo periodo);

- predisposizione di un certificato di analisi di rifiuti falso, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti - SISTRI; inserimento di un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti (art. 260-bis, co. 6);

- trasporto di rifiuti pericolosi senza copia cartacea della scheda SISTRI – Area movimentazione o del certificato analitico dei rifiuti, nonché uso di un certificato di analisi contenente false indicazioni circa i rifiuti trasportati in ambito SISTRI (art. 260-bis, co. 6 e 7, secondo e terzo periodo);

- trasporto di rifiuti con copia cartacea della scheda SISTRI – Area movimentazione fraudolentemente alterata (art. 260-bis, co. 8, primo e secondo periodo). La condotta di cui al co. 8, secondo periodo, è aggravata se riguarda rifiuti pericolosi;

8. Traffico illecito di rifiuti (artt. 259 e 260):

- spedizione di rifiuti costituente traffico illecito (art. 259, co. 1). La condotta è aggravata se riguarda rifiuti pericolosi;

- attività organizzate, mediante più operazioni e allestimento di mezzi e attività continuative, per il traffico illecito di rifiuti (art. 260). Delitto, caratterizzato da dolo specifico di ingiusto profitto e pluralità di condotte rilevanti (cessione, ricezione, trasporto, esportazione, importazione o gestione abusiva di ingenti quantitativi di rifiuti). La pena è aggravata in caso di rifiuti ad alta radioattività (co. 2);

9. Inquinamento atmosferico (art. 279);

- violazione, nell'esercizio di uno stabilimento, dei valori limite di emissione o delle prescrizioni stabiliti dall'autorizzazione, dai piani e programmi o dalla normativa, ovvero dall'autorità competente, che determini anche il

superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa (co. 5);

3. Reati previsti dalla Legge 7 febbraio 1992, n. 150 in materia di commercio internazionale di esemplari di flora e fauna in via di estinzione e detenzione animali pericolosi

10. importazione, esportazione, trasporto e utilizzo illeciti di specie animali (in assenza di valido certificato o licenza, o in contrasto con le prescrizioni dettate da tali provvedimenti);

11. detenzione, utilizzo per scopi di lucro, acquisto, vendita ed esposizione per la vendita o per fini commerciali di esemplari senza la prescritta documentazione; commercio illecito di piante riprodotte artificialmente (art. 1, co. 1 e 2 e art. 2, co. 1 e 2).

    Le condotte di cui agli artt. 1, co. 2, e 2, co. 2, sono aggravate nel caso di recidiva e di reato commesso nell'esercizio di attività di impresa.

12. falsificazione o alterazione di certificati e licenze; notifiche, comunicazioni o dichiarazioni false o alterate al fine di acquisire un certificato o una licenza; uso di certificati e licenze falsi o alterati per l'importazione di animali (art. 3-bis, co. 1);

13. detenzione di esemplari vivi di mammiferi e rettili di specie selvatica o riprodotti in cattività, che costituiscano pericolo per la salute e per l'incolumità pubblica (art. 6, co. 4);

4. Reati previsti dalla Legge 28 dicembre 1993, n. 549, in materia di tutela dell'ozono stratosferico e dell'ambiente

14. Inquinamento dell'ozono: violazione delle disposizioni che prevedono la cessazione e la riduzione dell'impiego (produzione, utilizzazione, commercializzazione, importazione ed esportazione) di sostanze nocive per lo strato di ozono (art. 3, co. 6);

5. Reati previsti dal D.Lgs. 6 novembre 2007, n. 202, in materia di inquinamento dell'ambiente marino provocato da navi

15. sversamento colposo in mare da navi di sostanze inquinanti (art. 9, co. 1 e 2);

16. sversamento doloso in mare da navi di sostanze inquinanti (art. 8, co. 1 e 2).

Le condotte di cui agli artt. 8, co. 2 e 9, co. 2 sono aggravate nel caso in cui la violazione provochi danni permanenti o di particolare gravità alla qualità delle acque, a specie animali o vegetali o a parti di queste.

Le sanzioni a carico dell'ente

Quanto alle sanzioni configurate a carico dell'ente, il legislatore delegato si è avvalso della facoltà conferitagli nella legge delega di non ricorrere necessariamente alle sanzioni interdittive previste dal D.Lgs. n. 231/2001.
L'applicazione di tali sanzioni, per una durata fissata dalla novella nella misura non superiore ai sei mesi, è stata infatti riservata soltanto ai casi in cui i reati da cui scaturisce la responsabilità dell'ente siano quelli previsti, rispettivamente:

1) dall'art. 137, commi 2, 5 secondo periodo, e 11 d. lgs. n. 152/2006;
2) dall'art. 256, comma 3 d. lgs. n. 152/2006;
3) dall'art. 260 d. lgs. n. 152/2006;
4) dagli artt. 8, commi 1 e 2, e 9, comma 2 d.lgs. n. 202/2007.

Solo in tali ipotesi, dunque, sarà possibile applicare alla persona giuridica le medesime sanzioni in via cautelare ai sensi degli artt. 45 e ss. del D.Lgs. n. 231/2001.
La novella ha previsto anche l'applicazione della sanzione più grave tra quelle previste dal D.Lgs. n. 231/2001, ovvero l'interdizione definitiva dall'esercizio dall'attività di cui all'art. 16, in due ipotesi, ovvero nel caso in cui l'ente o una sua attività organizzativa vengano stabilmente utilizzati allo scopo unico o prevalente di consentire od agevolare la commissione dei reati di:

a) “associazione” finalizzata al traffico illecito di rifiuti (art. 260 d. lgs. n. 152/2006);
b) sversamento in mare doloso di materie inquinanti (artt. 8, commi 1 e 2 d.lgs. n. 202/2007).

La sanzione pecuniaria è invece prevista in relazione a tutte le ipotesi per cui è stata configurata la responsabilità degli enti.
La stessa è stata diversamente articolata in proporzione alla diversa gravità dei reati presupposto cooptati nel catalogo di cui all’art. 25-undecies.
Nello specifico si avrà:

Uccisione, distruzione, cattura, prelievo e detenzione di esemplari di specie animali o vegetali selvatiche protette (fino a 387.250 €);

Distruzione o deterioramento di habitat all’interno di un sito protetto (da 38.700 a 387.250 €.

Scarichi idrici

- scarico di reflui industriali contenenti sostanze pericolose con valori superiori al limite o senza osservare le prescrizioni dell'autorizzazione (da 38.700 a 387.250 €);
- scarico di reflui industriali su suolo con valori superiori al limite (da 38.700 a 464.700 €);
- scarico non ammesso su suolo, negli strati superficiali del sottosuolo o nel sottosuolo (da 38.700 a 464.700 €).

Rifiuti

- attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti non autorizzate (fino a 464.700 €);
- violazione dei criteri di deposito temporaneo di rifiuti sanitari pericolosi (fino a 387.250 €);
- inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con superamento delle concentrazioni soglia di rischio (fino a 387.250 €);

- predisposizione ed uso di un certificato di analisi di rifiuti contenente false indicazioni (da 38.700 a 387.250 €);
- spedizione transfrontaliera di rifiuti costituente traffico illecito (da 38.700 a 387.250 €);
- attività organizzate per ingente traffico illecito di rifiuti (da 77.400 a 774.500 €, da 103.200 a 1.239.200 € per rifiuti radioattivi).

Emissioni in atmosfera

- superamento dei valori limite di emissione che provochi anche il superamento dei valori limite di qualità dell'aria (fino a 387.250 €).

Commercio di esemplari di specie protette (fino a 774.500 €).

Produzione o impiego di sostanze lesive dell'ozono stratosferico non ammesse (da 38.700 a 387.250 €)

Inquinamento provocato dalle navi (fino a 464.700 €).

La cornice edittale più significativa prevista dalla novella risulta dunque quella riservata alle attività organizzate per il traffico illecito di rifiuti di cui all'art. 260, comma 1 del codice dell'ambiente e la cui forbice è compresa tra il minimo di quattrocento e quello di ottocento quote, che, una volta determinato il valore della singola quota ai sensi dell'art. 10 D.Lgs. n. 231/2001, comporta in ipotesi l'irrogabilità di una sanzione pecuniaria massima pari ad 1.239.200 euro.
Le pene pecuniarie variano mediamente tra le centocinquanta e le duecentocinquanta quote e comportano l'irrogabilità di sanzioni che possono variare al più tra i 232.250 e i 387.250 euro.

LA REALIZZAZIONE DELLA PREVENZIONE DEI REATI AMBIENTALI IN SAN MARCO

LA REALIZZAZIONE DELLA PREVENZIONE DEI REATI AMBIENTALI IN SAN MARCO

L'elaborazione della risk analysis ambientale di SAN MARCO

Il team di lavoro dell'Istituto di Studi sulla responsabilità amministrativa degli enti ha condotto la risk analysis in SAN MARCO sulle tematiche ambientali seguendo la stessa metodologia percorsa per le atre aree di reato presupposto: la metodologia "top down". Anche in tal caso infatti non è apparso proficuo procedere ad una analisi delle attività dichiarate dall'ente in sede di audit per confrontarle con le disposizioni di legge.
Come già si era espresso nella Parte Generale infatti tale modo di procedere, tipico delle procedure di certificazione, non si adatta direttamente alle finalità di prevenzione dei reati specificamente posti dalla legge come presupposto di una responsabilità così grave come quella disciplinata da D.lgs. 231/2001, che coinvolge tutto l'ente quale responsabile penale.
La soluzione migliore per affrontare il tema della prevenzione è invece quella che prevede di considerare preliminarmente in astratto le condotte che possono generare il rischio di commissione di reato presupposto, inquadrarle nelle normali attività aziendali, e poi confrontarle nell'attività di audit con le contromisure in essere allo stato, e le eventuali azioni di miglioramento. Questo procedimento costituisce una valida guida per lo svolgimento dell'attività di audit ed una sicura base di partenza per commisurare correttamente l'entità e la tipologia delle azioni correttive necessarie.
Il team di ISR ha quindi preso in considerazione le fattispecie di reato introdotte dal D.lgs. 121/2011, individuando presso SAN MARCO le attività di funzione che possono essere interessate da un'azione deviante che arriva a realizzare la fattispecie incriminata.
In seguito a ciò il team di lavoro ha determinato il valore di rischio in astratto quindi ha proceduto successivamente alla attività di audit che ha consentito di verificare lo stato di attuazione delle norme di legge, delle disposizioni comunitarie e delle normative di certificazione in tema ambientale presso SAN MARCO
L'analisi condotta ha riguardato prevalentemente i seguenti settori:

1. gestione della filiera produttiva

2. gestione dei siti
3. gestione dei rifiuti
4. gestione delle immissioni nelle acque di reflui industriali
5. gestione delle immissioni di gas in atmosfera
6. gestione delle altre forme di immissioni (polveri, vibrazioni, rumori, scuotimenti)
7. gestione dei rapporti con le Autorità pubbliche in materia di comunicazioni, autorizzazioni, procedimenti accertatori e sanzionatori
8. gestione della documentazione

Le regole in linea generale

La risk analysis ha consentito di individuare le aree di attività sensibili non ancora coperte da disposizioni generali o procedurali che mettano gli operatori nelle condizioni di rispettare i dettami della normativa penale italiana e delle direttive europee, nonché le disposizioni conseguenti ai trattati internazionali sottoscritti e ratificati dall'Italia.
Ciò ha condotto ad emanare nella presente Parte Speciale 4 le regole generali di condotta che consentono di mantenere l'attività aziendale in linea con le suddette normative.

GESTIONE DELLA FILIERA PRODUTTIVA

La gestione della filiera produttiva interessa le attività di funzione relative all'approvvigionamento di materie prime che possono essere provenienti da fornitori non in linea con le normative nazionali o internazionali di tutela dell'ambiente.
Qualora si potesse dare la prova della conoscenza da parte di SAN MARCO della conoscenza di tali violazioni, e la scelta economica di tali fornitori fosse determinata in modo rilevante da queste condotte, si avrebbe la responsabilità a titolo di concorso nel reato. L'ipotesi non è da sottovalutare, in linea di principio: è infatti molto frequente che i fornitori vengano scelti sul mercato globale proprio per i costi molto contenuti, conoscendo in anticipo o potendo ragionevolmente supporre comportamenti molto disinvolti dei fornitori in materia di rispetto

dell'ambiente. Comportamenti che molto spesso assumono i contorni di condotte sanzionate penalmente, come avviene ad esempio nel caso della tutela degli habitat naturali, della tutela delle specie animali e vegetali in via di estinzione (di grande importanza nelle filiere dell'industria alimentare o dell'abbigliamento), della tutela del mare.
Tale controllo di filiera deve necessariamente esplicarsi attraverso una scelta di fornitori che non sia dettata unicamente dalla logica economica, ma si esplichi anche tenendo in considerazione, per il punteggio da assegnare ai soggetti presenti nella "lista fornitori qualificati", anche i criteri del rispetto delle norme poste a tutela dell'ambiente, attraverso parametri certi e di agevole allegazione.
Indispensabile inoltre una corretta contrattualizzazione di tali parametri, in modo da poter escludere un fornitore già nello svolgimento di una commessa, qualora si venisse a scoprire un comportamento che riveste i caratteri di un reato ambientale, prevedendo tale esito con una specifica clausola.
Di grande aiuto da questo punto di vista può essere la certificazione ISO 14001, sia per l'azienda sia per i fornitori, ed in parte anche la SA 8000, in quanto consentono di tenere sotto controllo attraverso specifiche procedure questi aspetti.
La materia non riguarda in alcun modo il lavoro di SAN MARCO dal momento che la sua filiera, se così si può dire, non contempla il ricorso a fornitori a rischio da questo punto di vista, anzi si riduce quasi completamente a forniture da parte di altre aziende del Gruppo.

GESTIONE DEI SITI

La gestione del sito produttivo assume la massima importanza per un corretto approccio alla prevenzione dei reati ambientali. Le materie interessate da una previsione di reato e connesse alla gestione dei siti produttivi sono riconnesse in prevalenza al tema dei rifiuti, in primis alla possibilità di realizzare in un proprio sito produttivo una discarica non autorizzata di rifiuti (art. 256 3° comma del Codice Ambiente), ma nondimeno attengono alla gestione complessiva della produzione, dei macchinari, delle infrastrutture.
L'ente deve poter dimostrare costantemente una corretta organizzazione

GESTIONE DEI RIFIUTI

Tutti i rifiuti prodotti presso i cantieri della società SAN MARCO, sia pericolosi che non, vengono smaltiti, a cura del subappaltatore incaricato del montaggio, secondo le modalità stabilite dalla legge vigente.

Per la gestione dei rifiuti l'azienda provvede sempre alla redazione del formulario e a conferire il rifiuto a ditte specializzate o eventualmente se previsto dalla propria autorizzazione ad effettuare il trasporto in conto proprio.

L'azienda conferisce i rifiuti solo a ditte autorizzate in conformità a quanto previsto dal D.lgs n°152 del 2006 e s.m.i. per l'effettuazione dello smaltimento o del recupero del rifiuto

L'art. 183 del D.Lgs 152/2006 definisce come "rifiuto" *qualsiasi sostanza od oggetto di cui il detentore si disfi o abbia l'intenzione o abbia l'obbligo di disfarsi.*

La gestione dei rifiuti perseguirà un obiettivo di minimizzazione della produzione, di recupero e di corretto smaltimento dei rifiuti prodotti all'interno del sito.

Per tutte le tipologie di rifiuti elencati prodotti in cantiere dalla società SAN MARCO si provvederà alla raccolta ed allo smaltimento nel rispetto delle normative in essere.

SAN MARCO provvederà inoltre a realizzare un deposito temporaneo dei rifiuti all'interno del cantiere con contenitori divisi per ogni tipologia di rifiuto ed applicherà una politica di sgombero dei rifiuti specifica per ogni categoria

Per quanto concerne lo stoccaggio dei suddetti rifiuti, che saranno oggetto di successivo smaltimento, verrà predisposta una zona idonea, limitrofa all'area di cantiere, dove i materiali possano essere stoccati separatamente in base alla tipologia del materiale/rifiuto. In caso di presenza di materiale che possa determinare infiltrazioni e contaminazioni del suolo, le aree di stoccaggio saranno dotate di teli impermeabili.

Per quanto riguarda eventuali rifiuti misti dell'attività di costruzione e demolizione, miscele bituminose e terre e rocce da scavo non pericolose verranno avviate a recupero e/o smaltimento presso impianti autorizzati nello stesso giorno della loro produzione

Al termine delle attività l'area sarà ripulita da ogni tipo di materiale residuo eventualmente rimasto sul terreno. A conclusione dei lavori si effettuerà un sopralluogo per la verifica della corretta pulizia delle aree di cantiere e si predisporrà apposito verbale di sopralluogo che sarà allegato alla relazione finale della gestione dei rifiuti e degli altri materiali di risulta

Il trasporto dei rifiuti dal cantiere verso l'esterno impone alla società la compilazione del formulario e la compilazione del registro carico-scarico dei rifiuti.

Il formulario di identificazione di cui all'art. 193 del D.Lgs. 152/06 s.m.i. verrà redatto in quattro esemplari, compilato, datato e firmato dal produttore dei rifiuti e controfirmate dal trasportatore che in tal modo dà atto di aver ricevuto i rifiuti. Una copia del formulario deve rimanere presso il produttore e le altre tre, controfirmate e datate in arrivo dal destinatario, sono acquisite una dal destinatario e due dal trasportatore, che provvede a trasmetterne una al predetto produttore dei rifiuti.

Le attività di raccolta, stoccaggio, recupero e smaltimento sono gestite da Ditte esterne autorizzate, rispettando le caratteristiche delle varie tipologie dei rifiuti soggetti a differenziazione. In presenza del trasportatore della Società, e prima che questo abbandoni il cantiere con il carico di rifiuti, deve essere compilato il formulario di identificazione, che serve ad accompagnare i rifiuti durante il trasporto dal produttore allo smaltitore

GESTIONE DELLE IMMISSIONI DI REFLUI INDUSTRIALI NELLE ACQUE

Le attività di cantiere danno origine a reflui liquidi, che possono caratterizzarsi come inquinanti nei confronti dei recettori nei quali confluiscono. Le acque di cantiere hanno caratteristiche chimico-fisiche particolari, determinate dalle attività che le generano, e che non possono, generalmente, essere sversate in

un corpo recettore senza preventivo trattamento o comunque un'attenta valutazione.

Tali acque non possono essere quindi scaricate, di norma, nei recettori dedicati senza preventivo trattamento. In particolare non possono essere versate nelle acque superficiali (fiumi, canali scoli e fossi), né lasciate a dispersione nel terreno in quanto possono generare un impatto negativo sugli ecosistemi fluviali (variazioni della limpidezza delle acque, del pH, della composizione chimica) o sulle falde sotterranee.

In caso di scarico in fognature, dovrà essere preventivamente verificata la destinazione finale della rete e le capacità di depurazione degli impianti.

Il cantiere edile, inoltre, è un grande consumatore di risorse idriche, necessitando di acqua in grandi quantitativi per, ad esempio, la preparazione delle malte cementizie e dei conglomerati, la diluzione di fanghi bentonitici e polimerici, il lavaggio delle botti delle betoniere, il lavaggio dei mezzi d'opera e l'abbattimento delle polveri di cantiere.
Sono pertanto necessari accorgimenti per la limitazione del consumo di acqua, inoltre, dovranno essere evitati ristagni o accumuli non impermeabilizzati onde evitare la percolazione nel suolo di acque potenzialmente inquinate

Si rende indispensabile inoltre definire le modalità di prevenzione e controllo degli eventi di spillamento, trafilamento, traboccamento o rilascio accidentale di sostanze inquinanti, in quantità limitata, che potrebbe verificarsi per cause accidentali durante lo svolgimento delle attività di cantiere. Il presente documento dovrà essere distribuito dal Responsabile di cantiere a tutti gli addetti interessati. Tutto il personale coinvolto dovrà osservare il presente documento. La responsabilità della consulenza sull'interpretazione e l'utilizzo di questa Istruzione di Lavoro è dell'Addetto alla Sicurezza di Cantiere.
In caso di emergenze dovute al rinvenimento sostanze anomale in cantiere non prodotte dall'attività di cantiere stessa la società SAN MARCO provvederà immediatamente a segnalare il fatto alla Direzione Lavori e al Committente. Inoltre sarà a disposizione per tutti gli interventi previsti dalla normativa vigente. A tal riguardo manterrà attivo un contratto con una società specializzata in smaltimento rifiuti speciali.

GESTIONE DELLE IMMISSIONI DI GAS IN ATMOSFERA

Tutti gli strumenti e macchinari utilizzati dovranno essere conformi alle norme vigenti in materia di emissioni derivanti dalla combustione e mantenuti sempre in condizioni di perfetta efficienza.

GESTIONE DELLE ALTRE FORME DI IMMISSIONI (POLVERI, VIBRAZIONI, RUMORI, SCUOTIMENTI)

Tutte le lavorazioni dovranno essere svolte con modalità tali da limitare al minimo sollevamenti ed emissioni di polveri; dovranno comunque essere previsti adeguati sistemi di contenimento; in caso di necessità potranno essere effettuate bagnature del suolo e delle zone di lavoro

Tutti gli strumenti e macchinari utilizzati dovranno essere conformi alle norme vigenti in materia.

I limiti per le emissioni sonore diurne/notturne sono definiti dal Piano di Classificazione Acustica del territorio comunale, per eventuali superamenti di tali limiti dovrà essere fatta richiesta di superamento in deroga.

Le attività di cantiere possono generare impatti significativi sul suolo e sul sottosuolo, nonché sulle acque sotterranee, in particolare si segnala il rischio potenziale di contaminazione del terreno determinato da: versamenti accidentali di carburanti e lubrificanti; percolazione nel terreno di acque di lavaggio o di betonaggio; interramento di rifiuti o di detriti e dispersione di rifiuti pericolosi da demolizione.
La mitigazione degli impatti e la prevenzione dell'inquinamento potenziale si attua prevalentemente mediante provvedimenti di carattere logistico, quali, ad esempio, lo stoccaggio dei lubrificanti e degli oli esausti in appositi contenitori dotati di vasche di contenimento.

GESTIONE DEI RAPPORTI CON LE AUTORITÀ PUBBLICHE IN MATERIA DI COMUNICAZIONI, AUTORIZZAZIONI, PROCEDIMENTI ACCERTATORI E SANZIONATORI

I rapporti con tali autorità devono mantenersi nell'alveo della più assoluta correttezza, giacché le sanzioni conseguenti alla commissione di reati contro la Pubblica Amministrazione potrebbero sommarsi a quelle previste per la commissione di reati ambientali, aggravando considerevolmente la posizione dell'ente.
Si devono quindi considerare qui riportate le regole generali a le procedure specifiche previste nella Parte Speciale 1 del presente manuale, con particolare riferimento ai rapporti con i Pubblici Ufficiali ed alle dichiarazioni svolte nei confronti della Pubblica Autorità.
Tutti i rapporti che abbiano ad oggetto dichiarazioni, comunicazioni, richieste di autorizzazioni, procedimenti accertatori e sanzionatori, devono quindi essere condotti in modo rigorosamente aderente alle procedure aziendali di SAN MARCO, e devono comunque osservare le seguenti prescrizioni.
I seguenti principi di carattere generale si applicano, in via diretta, ai Dipendenti e agli Organi Societari di SAN MARCO e, in forza di apposite clausole contrattuali, ai Consulenti ed ai Partner.
E' fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, considerati singolarmente o complessivamente, siano idonei ad integrare le fattispecie di reato rientranti tra quelle considerate nella Parte Speciale 1 (Reati nei rapporti con la Pubblica Amministrazione: artt. 24 e 25 del D.Lgs. 231/01). Sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale 1.
Nell'ambito dei suddetti comportamenti è fatto divieto in particolare di:
a) effettuare elargizioni in denaro a pubblici funzionari o incaricati di pubblico servizio italiani o stranieri, nell'ambito dei rapporti inerenti dichiarazioni, comunicazioni, richieste di autorizzazioni, procedimenti accertatori e sanzionatori in tema di tutela ambientale.
b) offrire doni o gratuite prestazioni di qualsiasi tipo o natura, comunque rivolto ad acquisire trattamenti di favore nella conduzione di attività aziendale inerente dichiarazioni, comunicazioni, richieste di autorizzazioni, procedimenti accertatori e sanzionatori.
In particolare, ai rappresentanti della P.A. o a loro familiari non devono essere offerti, né direttamente né indirettamente, qualsiasi regalo, doni o gratuite

prestazioni che possano essere o, comunque, apparire connessi con il rapporto di affari con la società o miranti ad influenzare l'indipendenza di giudizio o indurre ad assicurare un vantaggio per la società stessa nell'ambito di dichiarazioni, comunicazioni, richieste di autorizzazioni, procedimenti accertatori e sanzionatori.
Le spese di cortesia in occasione di ricorrenze o, comunque, attinenti la sfera dell'immagine e della comunicazione, ivi comprese le sponsorizzazioni, non possono mai essere autorizzate dalla Direzione nei casi suddetti e nei confronti di Pubblici Ufficiali che abbiano funzioni in tal senso;
c) accordare, direttamente o indirettamente, vantaggi di qualsiasi natura in favore di rappresentanti della Pubblica Amministrazione italiana o straniera tali (o effettuati con modalità tali da) costituire una violazione dei principi esposti nel Modello;
d) eseguire prestazioni e riconoscere compensi in favore dei Consulenti o dei Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
e) presentare dichiarazioni non veritiere ad organismi pubblici nazionali, comunitari e internazionali al fine di conseguire vantaggi nell'ambito di dichiarazioni, comunicazioni, richieste di autorizzazioni, procedimenti accertatori e sanzionatori in materia ambientale.

GESTIONE DELLA DOCUMENTAZIONE

La corretta tenuta della documentazione è essenziale prima di tutto per un approccio efficace alla prevenzione dei reati presupposto e per garantire la migliore gestione dei fornitori e delle materie prime, dei siti, dei rifiuti e degli scarichi.
L'utilità si rivela altresì nella situazione degli accertamenti e dei procedimenti sanzionatori, allorquando diviene indispensabile poter produrre una completa dimostrazione della correttezza dell'approccio ai temi della prevenzione dei reati ambientali.
La miglior prassi in circolazione è quella relativa alla normativa di certificazione ISO 14001, che pone dei requisiti ed un sistema di gestione della documentazione ambientale sicuro ed affidabile. Per questo il Modello

Organizzativo di SAN MARCO deve tenere in considerazione le normative di certificazione UNI in materia di tenuta della documentazione.
La direzione dell'organizzazione dovrebbe definire la documentazione, registrazioni incluse, necessaria per stabilire, attuare e tenere aggiornato il sistema di gestione anche per l'ambiente e per sostenere un'efficace ed efficiente operatività dei processi dell'organizzazione.
Natura ed estensione della documentazione dovrebbero soddisfare i requisiti contrattuali, quelli cogenti nonché le esigenze e le aspettative del cliente e delle altre parti interessate ed essere adeguate all'organizzazione stessa. La documentazione può presentarsi in ogni forma o supporto rispondente alle esigenze dell'organizzazione.
Per produrre documentazione che soddisfi le esigenze e le aspettative delle parti interessate, la direzione dovrebbe prendere in esame:
- i requisiti contrattuali stabiliti dal cliente e dalle altre parti interessate,
- l'adozione di norme internazionali, nazionali, regionali e settoriali,
- i requisiti di tipo cogente applicabili,
- le decisioni prese dall'organizzazione,
- le fonti informative esterne attinenti allo sviluppo delle competenze dell'organizzazione,
- le informazioni sulle esigenze e aspettative delle parti interessate.

La preparazione, l'utilizzazione e la tenuta sotto controllo della documentazione dovrebbero essere valutate in funzione dell'efficacia e dell'efficienza dell'organizzazione a fronte di criteri quali:
- la funzionalità (come i tempi di transito dei processi),
- il rapporto amichevole con gli utilizzatori,
- le risorse necessarie,
- le politiche e gli obiettivi,
- i requisiti, presenti e futuri, relativi alle conoscenze di tipo gestionale,
- il confronto con i migliori sistemi di documentazione,
- le interfacce utilizzate dai clienti (dell'organizzazione), dai fornitori e dalle altre parti interessate.

Dovrebbe essere assicurato l'accesso alla documentazione al personale dell'organizzazione ed alle altre parti interessate, coerentemente con la politica per la comunicazione adottata dall'organizzazione

L’applicazione delle regole e l’implementazione delle azioni di sistema

Le aree di processo e le schede di controllo già implementate per l’analisi del rischio degli altri reati presupposto sono state revisionate nella struttura, comprendendo le sanzioni indicate dalla normativa in tema di protezione dell’ambiente.
Le ipotesi di sanzione misurate con lo strumento dinamico risultano quindi proporzionalmente aumentate di gravità, nella misura in cui la fase di audit abbia rilevato un pericolo di commissione dei reati presupposto che possono portare ad una condotta tipica.

All’applicazione delle normative introdotte con il D.lgs. 121/2011 è stata quindi dedicata una specifica Area di Processo, che permette di identificare le attività sensibili e valutare costantemente le necessarie azioni correttive, misurando la pericolosità delle singole funzioni interessate in organigramma, in relazione alle attività svolte.

Parte Speciale 6: DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

Considerazioni generali

La Legge n. 48/2008 ha integrato nuovamente l'area dei reati presupposto in presenza dei quali scatta la responsabilità degli enti: all'art. 24-bis, figurano alcuni dei comportamenti che rappresentano minacce alla sicurezza informatica e che, nel nostro ordinamento, sono qualificati come condotte penalmente rilevanti.

La sicurezza informatica si interfaccia con la tutela dei dati personali al punto che, lo stesso Codice Privacy (D.lgs. n.196/03), in tema di tutela dei dati personali, stabilisce obblighi specifici e generali che si sostanziano nella necessità, da parte del titolare del trattamento dei dati, di implementare una serie di misure minime di sicurezza identificate direttamente dalla normativa, oltreché misure idonee e preventive da identificare in base ad un'accurata analisi dei rischi.

Le misure minime di sicurezza, di cui all'Allegato B al Codice Privacy, stabiliscono il livello minimo di protezione dei dati e la loro adozione è *conditio sine qua non* per lo svolgimento delle attività di trattamento dei dati.

All'interno dell'azienda, i rischi correlati al crimine informatico sono di grande rilevanza; si pensi che la maggior parte dei processi aziendali sono informatizzati e per di più esternalizzati; l'assistenza tecnica od i servizi di cloud computing ne sono un chiaro esempio.

A questo proposito, il d.lgs. 231 prevede che tra l'autore materiale del reato e l'ente non debba intercorrere necessariamente un rapporto di lavoro subordinato, rilevando la subordinazione alla direzione o vigilanza di uno dei soggetti in posizione apicale, la quale è rinvenibile anche nei rapporti con i collaboratori esterni/consulenti.

Questi ultimi devono essere nominati responsabili del trattamento, come nel caso dell'amministratore di sistema in outsourcing, del fornitore di servizi cloud o del manutentore del sito web aziendale e come tali devono attenersi, secondo quanto prescritto dallo stesso Codice Privacy all'art. 29, alle istruzioni loro fornite dal titolare. È rinvenibile in tali rapporti quel vincolo di subordinazione alla vigilanza

e direzione dei soggetti apicali, richiesto dall'art. 5 del D.lgs. 231, per l'insorgere della responsabilità amministrativa dell'ente.

In particolare, le aziende devono valutare ex ante l'affidabilità di tali consulenti/fornitori nonché prevedere, nei contratti conclusi con gli stessi, un'apposita clausola che regoli le conseguenze delle violazioni alle norme del D.lgs. 231/01.

La prevenzione dei reati informatici, al fine di evitare di incorrere nella citata responsabilità, passa attraverso la predisposizione di misure di sicurezza fisica, logica ed organizzativa. La sensibilizzazione della dirigenza e dei dipendenti, la loro formazione, le azioni di monitoraggio ed audit sono solo alcuni dei punti chiave per assicurare l'azienda dalle gravi ripercussioni previste dal D.lgs. 231/01.

Per difendersi l'azienda ha vari strumenti che riducono il rischio di commissione di reati ed illeciti, i più efficaci dei quali sono l'adozione di un valido ed efficace modello di organizzazione e gestione e di una privacy policy.

Il rispetto della normativa privacy, prevedendo l'applicazione di misure minime di sicurezza, consente appunto di prevenire la commissione dei reati presupposti previsti dal D.lgs. 231/01; le policy ed i modelli organizzativi sono efficaci ed assumono valore esimente, solamente se concretamente attuati e se portati a conoscenza di dipendenti e stakeholder.

L'art. 24 bis D.lgs. 231/2001

Delitti informatici e trattamento illecito di dati

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

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

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

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

Il significato dell'art. 24 bis: fattispecie e conseguenze

LA CONDOTTA TIPICA

L'accesso abusivo punisce la condotta di chi si introduce abusivamente – ossia eludendo una qualsiasi forma, anche minima, di barriere ostative all'accesso – in un sistema informatico o telematico, protetto da misure di sicurezza, rimanendovi contro la volontà di chi ha diritto di escluderlo.
Due sono pertanto le condotte penalmente rilevanti: l'intrusione in un sistema protetto ed il mantenimento nello stesso contro la volontà espressa o tacita di chi ha il diritto di esclusione. Di conseguenza si parla di accesso abusivo sia nel caso in cui il soggetto, pur legittimato all'utilizzo del sistema, entri in ambienti informatici a cui non è autorizzato ad accedere, sia nel caso in cui lo stesso, pur essendo abilitato, acceda o si mantenga nel sistema violando le condizioni ed i limiti fissati dal titolare per delimitarne oggettivamente l'accesso, restando invece del tutto irrilevanti le finalità che hanno mosso l'agente.
Perché il reato si configuri il sistema deve essere protetto da misure di sicurezza. Occorre dunque dimostrare che siano stati adottati dei meccanismi di selezione dei soggetti abilitati all'accesso del sistema informatico che possono essere di

tipo logico (es. firewall, password, codici d'accesso, dati biometrici), fisico (es. sistemi di videosorveglianza, porte blindate) od organizzativo (es. accesso ai locali vietato al personale impiegatizio).
E' sufficiente che il soggetto agisca con la coscienza e la volontà di introdursi nell'altrui sistema protetto ovvero di rimanervi contro la volontà di chi ha diritto di escluderlo, mentre non rilevano in alcun modo le finalità (curiosità, ricerca di informazioni riservate, intento vandalico o manipolativo) per cui il soggetto agisce.Oggetto di tutela è il "domicilio informatico" quale spazio fisico e ideale, estensione della sfera di riservatezza della persona (sia fisica che giuridica).

SOGGETTO AGENTE

E' un reato che può essere compiuto da chiunque abbia accesso al sistema, per cui può essere realizzato tanto dall'utente generico quanto dall'amministratore di sistema (magari in outsourcing). Dal momento che non esistono delle aree o funzioni maggiormente a rischio si rileva la necessità di una vigilanza "trasversale".

IL PRESUPPOSTO 231

Posto che ai sensi del d.lgs.231/01 il reato deve essere commesso "nell'interesse o a vantaggio" dell'azienda per fondare una responsabilità della stessa, si avrà accesso abusivo, rilevante in chiave 231, a titolo esemplificativo, allorquando il soggetto (apicale o sottoposto) acceda abusivamente al sistema di un'azienda concorrente al fine di conoscerne il portafoglio clienti o per acquisire, a scopo di spionaggio industriale, la documentazione relativa ai suoi prodotti. Si avrà altresì accesso abusivo anche quando il soggetto acceda abusivamente ai propri sistemi informatici, ad esempio per manipolarne i dati al fine di ottenere un vantaggio in ordine agli adempimenti contabili e di bilancio.

Come. In generale, costituiscono attività "sensibili" (i.e. a rischio di commissione di reato) tutti gli accessi ai sistemi informatici/telematici.

LA PREVENZIONE DEL MODELLO ORGANIZZATIVO

Tra i protocolli da adottare per prevenire la commissione di questa tipologia di reato, fondamentale è il ricorso ad adeguate policies (supportate da corrispondenti procedure) che andranno a disciplinare la gestione degli account e dei profili di autorizzazione, la gestione della rete aziendale e di internet nonché l'utilizzo della posta elettronica.

LE SANZIONI

La sanzione prevista è quella pecuniaria da cento a cinquecento quote (in grado dunque di arrivare sino ad € 774.500) nonché, laddove ricorrano le condizioni di cui agli artt. 9, 12 e 13, d.lgs. 231/01, le sanzioni interdittive dell´interdizione dall'esercizio dell´attività, della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

I reati presupposto

Art. 615-ter c.p. - Accesso abusivo ad un sistema informatico o telematico.
«Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della
qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o i danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni».

L'oggetto giuridico tutelato dalla norma è, secondo la teoria predominante, il "domicilio informatico".
Per sistema informatico o telematico deve intendersi "un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente" (Cass. 3067/1999).
Il sistema informatico, dovendo svolgere una funzione - mediante tecnologie informatiche - è dunque tale se gestisce o elabora dati, mentre tutto ciò che, in un sito web o nel mondo dell'informatica, non è capace di gestire o elaborare dati in vista dello svolgimento di una funzione non è "sistema informatico".
La mera copiatura dei contenuti di un sito, realizzata semplicemente dalla visualizzazione del sito senza introduzione nella "memoria interna" del sito o nei programmi che ne consentono il funzionamento, non concreta interazioni con il sistema informatico come definito dalla giurisprudenza; peraltro, si segnala che la norma in questione è stata introdotta al fine di reprimere il fenomeno degli hacker, cosa ben diversa dalla consultazione / visualizzazione / copiatura del contenuto di una pagina web.
Dirimente ai fini della configurabilità del reato è la presenza o meno delle cd. misure di sicurezza nel sistema informatico / telematico.
Sono tali quelle protezioni (che possono essere apposte sia a livello di apparecchiature (hardware) che di programmi (software) che integrano quei

peculiari meccanismi operativi che impediscono un libero accesso al sistema e, quindi, la presa di cognizione di informazioni e dati ivi rinvenibili) a terzi estranei (ad esempio, codice alfanumerico di accesso, chiave di avviamento, eccetera.
L'apposizione di siffatte misure protettive del sistema informatico o telematico costituisce, infatti, l'estrinsecazione della voluntas excludendi manifestata dal titolare del relativo ius.
L'accesso ad un sistema non protetto, pertanto, risulta atipico e penalmente lecito ma non anche civilisticamente, dovendosi, a tale riguardo, ulteriormente verificare in concreto un danno ingiusto risarcibile ex articolo 2043 CC.
La Corte di Cassazione ha aderito all'orientamento interpretativo estensivo dell'art. 615-ter parte seconda e stabilito la configurabilità del reato "nel caso in cui il soggetto legittimato all'accesso per motivi di servizio o di ufficio s'introduca per motivi diversi".

Art. 617 - quater c.p. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.
«Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.
Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:
- in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- da chi esercita anche abusivamente la professione di investigatore privato».

Tale norma mira a impedire l'intercettazione fraudolenta, ravvisabile ogniqualvolta l'agente prenda conoscenza delle comunicazioni in maniera occulta e senza essere legittimato.
La Cassazione ha statuito che integra la violazione di cui all'art. 617-quater, comma 2 c.p., la condotta di chi diffonda al pubblico una trasmissione televisiva interna, trasmessa da punto a punto (cd "fuori onda") su un canale riservato a comunicazioni di servizio e intercettata in modo fraudolento. Il caso si riferiva a Striscia la notizia che aveva "intercettato" dei fuori onda e poi trasmessi nel corso della propria trasmissione.

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

Tale norma è volta a sanzionare la semplice predisposizione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche.
Va segnalata una pronuncia del GIP presso il Tribunale di Milano secondo cui integra il reato di cui all'art. 617- quinquies c.p. e non il reato di cui all'art. 615-quater c.p. la condotta di chi installa su uno sportello bancomat, in sostituzione del pannello originario, una apparecchiatura composta da una superficie plastificata, con una microtelecamera con funzioni di registratore video per la rilevazione dei codici bancomat, quando non vi sia prova certa dell'avvenuta captazione di almeno un codice identificativo.
L'attività illecita d'intercettazione, infatti, nel silenzio dell'art. 617- quinquies c.p., deve ritenersi possa essere consumata con qualunque mezzo ritenuto idoneo a svelare la conoscenza di un sistema informatico qual è da considerarsi la digitazione da parte dell'operatore umano del codice di accesso ad un sistema

attraverso una tastiera alfanumerica, digitazione che era destinata ad essere l'oggetto dell'illecita captazione.

Art. 635-bis c.p. – Danneggiamento di informazioni, dati e programmi informatici.
«Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio».
Art. 635 c.p. - Danneggiamento
"Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui è punito, a querela della persona offesa con la reclusione fino a un anno o con la multa fino a lire seicentomila.
La pena è della reclusione da sei mesi a tre anni e si procede d'ufficio, se il fatto è commesso:
1)con violenza alla persona o con minaccia;
(omissis)

L'art. 635-bis non si limita ad ampliare ed integrare la norma sul danneggiamento (art. 635 c.p.), con riguardo ai dati ed ai programmi, ossia alle componenti immateriali di un sistema informatico, ma predispone altresì una tutela rafforzata di tutti i beni informatici, prevedendo un trattamento più rigoroso, sia sotto il profilo sanzionatorio che sotto il profilo della procedibilità, anche di fatti che erano pacificamente riconducibili alla fattispecie tradizionale, in quanto aventi ad oggetto cose materiali: il sistema informatico o telematico, ovvero il supporto materiale delle informazioni.
Oggetto di danneggiamento può essere innanzitutto il sistema informatico, eventualmente collegato a distanza con altri elaboratori, come nel caso dei sistemi telematici e l'aggressione può riguardare tanto il sistema nel suo complesso quanto una o più delle sue componenti materiali, quali il video, la tastiera, etc.
Il danneggiamento, inoltre, può riguardare anche i dati e i programmi informatici nonché le informazioni contenute nel sistema.

L'art. 635 bis richiede che i beni informatici oggetto di aggressione siano «altrui»: il problema del significato da attribuire a tale termine sembra destinato ad assumere rilevanza pratica proprio in relazione alla nuova figura di danneggiamento informatico, stante la diffusa prassi di procurarsi la disponibilità di hardware e di software attraverso contratti di locazione (anziché di compravendita), solitamente accompagnati dalla contestuale conclusione di un contratto di assistenza e/o manutenzione con lo stesso fornitore.
Il danneggiamento si può attuare nella distruzione e nel deterioramento e nell'inservibilità totale o parziale.

Art. 635-ter c.p. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.
«Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.
Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata».

La prevenzione dei reati presupposto in SAN MARCO

Nell'espletamento di tutte le operazioni attinenti alla gestione e all'utilizzo dei sistemi informativi aziendali, i Dipendenti e gli Organi Sociali devono adottare e rispettare:

1. il sistema di controllo interno, e quindi le procedure aziendali, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale e organizzativa;
2. le norme inerenti la gestione e l'utilizzo dei sistemi informativi di SAN MARCO ;
3. il sistema disciplinare;
4. in generale, la normativa applicabile.

Si precisa che SAN MARCO ha delegato ad un provider terzo la gestione dei sistemi informativi aziendali, l'implementazione, il monitoraggio e la corretta applicazione delle relative procedure di controllo, disciplinando compiutamente gli aspetti relativi a condizioni e modalità di erogazione del servizio all'interno di uno specifico contratto di service (si veda al riguardo anche quanto espressamente previsto dal successivo paragrafo).

In virtù degli accordi contrattuali in essere tra le parti, al fine di presidiare l'attività sensibile in oggetto, il service provider, su indicazioni specifiche di SAN MARCO , adotta tutte le misure di cui al successivo paragrafo, garantendo piena conformità dei servizi erogati rispetto ai criteri stabiliti all'interno dei contratti ed essendo pertanto responsabile di eventuali inadempienze.

3.2 PRINCIPI GENERALI DI COMPORTAMENTO

La presente parte speciale prevede l'espresso divieto a carico degli Organi Sociali (in via diretta) e dei lavoratori dipendenti e dei consulenti di SAN MARCO (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

• 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 considerate (art. 24-bis del d.lgs. 231/2001);
• violare i principi e le procedure aziendali previste nella presente parte speciale.

La presente Parte Speciale comporta, conseguentemente, l'obbligo a carico dei soggetti sopra indicati di rispettare scrupolosamente tutte le leggi vigenti ed in particolare di:

1. impegnarsi a non rendere pubbliche tutte le informazioni loro assegnate per l'utilizzo delle risorse informatiche e l'accesso a dati e sistemi (avuto particolare riguardo allo username ed alla password, anche se superata, necessaria per l'accesso ai sistemi dell'Azienda);

2. attivare ogni misura ritenuta necessaria per la protezione del sistema, evitando che terzi possano avere accesso allo stesso in caso di allontanamento dalla postazione (uscita dal sistema o blocco dell'accesso tramite password);
3. accedere ai sistemi informativi unicamente a mezzo dei codici identificativi assegnati al singolo soggetto e provvedere, entro le scadenze indicate dal Responsabile ICT Governance, alla modifica periodica della password;
4. astenersi dal porre in essere qualsivoglia comportamento che possa mettere a rischio la riservatezza e/o l'integrità dei dati aziendali;
5. assicurare la veridicità delle informazioni contenute in qualsivoglia atto e/o documento informatico.
Nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di: a) intraprendere azioni atte a superare le protezioni applicate ai sistemi informativi aziendali;
b) installare alcun programma, anche se attinente all'attività aziendale, senza aver prima interpellato il Responsabile ICT Governance;
c) accedere alla rete aziendale, attraverso una connessione alternativa rispetto a quella messa a disposizione da parte dell'Azienda, al fine di eludere il sistema di accesso protetto implementato;
d) accedere in maniera non autorizzata ai sistemi informativi di terzi, né alterarne in alcun modo il loro funzionamento, al fine di ottenere e/o modificare, senza diritto, dati, programmi o informazioni;

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.), identificate anche in funzione di specifici criteri di importo e significatività della fornitura e coinvolte nello svolgimento di attività a rischio rispetto ai delitti informatici e trattamento illecito di dati e che operano per conto o nell'interesse di SAN MARCO , i relativi contratti, secondo precisi criteri di selezione definiti nel presente Modello, devono:
• essere definiti per iscritto, in tutte loro condizioni e termini;
• contenere clausole standard al fine del rispetto del D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto);
• contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D. Lgs. 231/2001 (ovvero, se si tratta di

soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto) e di impegnarsi a tenere comportamenti conformi al dettato della norma;
• contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto) (es. clausole risolutive espresse, penali).

4. LE "ATTIVITÀ SENSIBILI RELATIVE AI DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI" AI FINI DEL D.LGS. 231/2001

Le attività sensibili individuate, in riferimento ai Delitti informatici e di trattamento illecito di dati richiamati dall'art. 24-bis del d.lgs. 231/2001, sono le seguenti:
- Utilizzo di risorse e informazioni di natura informatica o telematica, ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore (con particolare riferimento alle occasioni di reato "Gestione delle informazioni relative all'accesso alle risorse informatiche, ai dati ed ai sistemi info-telematici" e "Invio telematico di atti, documenti e scritture").

5. PRINCIPI GENERALI DI CONTROLLO

I Principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzati come segue:
• SEGREGAZIONE DELLE ATTIVITÀ: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
• ESISTENZA DI PROCEDURE/NORME/CIRCOLARI: devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
• POTERI AUTORIZZATIVI E DI FIRMA: i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere chiaramente definiti e conosciuti all'interno della Società;

• TRACCIABILITÀ: ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

6. PRINCIPI DI RIFERIMENTO SPECIFICI RELATIVI ALLE REGOLAMENTAZIONE DELLE SINGOLE ATTIVITÀ SENSIBILI

Ai fini dell'attuazione delle regole elencate al precedente capitolo 3, oltre che dei principi generali contenuti nella parte generale del presente Modello e dei principi generali di controllo di cui al capitolo 5, nel disciplinare le Fattispecie di attività sensibili di seguito descritta, dovranno essere osservati anche i seguenti principi di riferimento.

6.1 UTILIZZO DI RISORSE E INFORMAZIONI DI NATURA INFORMATICA O TELEMATICA OVVERO DI QUALSIASI ALTRA OPERA DELL'INGEGNO PROTETTA DA DIRITTO D'AUTORE

La regolamentazione dell'attività deve prevedere:

• l'implementazione di un approccio di governance dei sistemi informativi aziendali improntato al rispetto degli standard di sicurezza attiva e passiva, volti a garantire l'identità degli utenti e la protezione, la confidenzialità, l'integrità e la disponibilità dei dati. In particolare SAN MARCO ha implementato un sistema centralizzato per la gestione delle componenti software, che, pertanto, non possono essere aggiornate o modificate in alcun modo da parte del singolo utente;

• la possibilità di accedere ai sistemi informativi solo previa opportuna identificazione da parte dell'utente, a mezzo username e password assegnati originariamente dall'Azienda. Per i sistemi di identificazione e accesso SAN MARCO ha definito un iter tale per cui ogni utente ha necessità di inserire una password - costituita da un codice alfanumerico con un numero minimo di caratteri - per "loggarsi" e accedere ai sistemi;

• l'obbligo di cambiamento della password, a seguito del primo accesso, e la periodicità di modifica della suddetta password a seconda della frequenza di utilizzo e della criticità dei dati cui si accede per mezzo della stessa. In particolare il sistema informativo di SAN MARCO prevede che ciascun utente modifichi la

propria password periodicamente e comunque non oltre 60 giorni dalla registrazione. Qualora l'utente non provveda alla modifica di propria iniziativa, il sistema è strutturato in modo da inviare in automatico alert preliminari alcuni giorni prima che la password scada. Decorso anche questo termine, il sistema obbliga l'utente al cambio password per poter accedere al sistema; il monitoraggio, con frequenza periodica, di tutti gli accessi e le attività svolte sulla rete aziendale nei limiti e con le modalità di cui alla vigente normativa.
SAN MARCO prevede una lista con un elenco dettagliato di siti inaccessibili ai propri utenti;
• la registrazione e la verifica di tutti gli accessi e le attività svolte sulla rete aziendale da remoto, nei limiti e con le modalità di cui alla vigente normativa. In particolare gli utenti autorizzati da SAN MARCO hanno la possibilità di accedere alla rete da remoto tramite check-point VPN - previa espressa autorizzazione del Responsabile gerarchico, oppure utilizzando esclusivamente la mail, con l'autorizzazione del Responsabile gerarchico e dopo aver seguito un corso sulla sicurezza informatica;
• Inoltre il Responsabile del Personale comunica tutte le assunzioni e le cessazioni, nonché tutti i passaggi di stato/mansioni che possono impattare sulla gestione delle utenze informatiche, in modo che vengano attivate tutte le utenze necessarie. Si sottolinea che, al fine di abilitare le utenze, è necessaria l'autorizzazione del diretto superiore dell'utente richiedente.
La cessazione dei rapporti lavorativi comportano la disattivazione delle utenze. E' previsto in ogni caso che, decorsi 60 giorni dalla data di ultimo utilizzo, le utenze vengano comunque disattivate;
• l'adeguata formazione di ogni risorsa sui comportamenti da tenere per garantire la sicurezza dei sistemi informativi e sulle possibili conseguenze, anche penali, che possono derivare dalla commissione di un illecito.

7. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

Fermo restando il potere discrezionale di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività di SAN MARCO potenzialmente a rischio di compimento dei Delitti informatici e di trattamento illecito di dati che sono state incluse nel piano di lavoro approvato dall'Organismo stesso, in funzione della valutazione del rischio assegnata in sede di predisposizione del Modello e nel corso dei suoi successivi aggiornamenti (si veda al riguardo l'Allegato 1 al presente documento). Tali controlli sono diretti a verificare la conformità dei

comportamenti in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.
A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le Fattispecie di attività sensibili. L'Organismo di Vigilanza riferisce di detti controlli al Organismo di Gestione.

PARTE SPECIALE 7

PRIVACY E DATA PROTECTION

LE REGOLE DEL MODELLO 231 NELLA DISCIPLINA GDPR

INQUADRAMENTO GENERALE DELLA NORMATIVA

Il General Data Protection Regulation (GDPR), ovvero il Regolamento UE n. 679/2016 sulla protezione dei dati personali (o Regolamento sulla privacy), è entrato in vigore Il 24 maggio 2016, per divenire pienamente applicabile dal 25 maggio 2018, abrogando la Direttiva 95/46/CE.[5]
Il testo affronta anche il tema dell'esportazione di dati personali al di fuori dell'UE e obbliga tutti i Titolari del trattamento dei dati (anche con sede legale fuori dall'Unione Europea) che trattano dati di residenti nell'unione europea ad osservare ed adempiere agli obblighi previsti. Gli obiettivi principali della Commissione europea nel GDPR sono quelli di restituire ai cittadini il controllo dei propri dati personali e di semplificare il contesto normativo che riguarda gli affari internazionali unificando e rendendo omogenea la normativa privacy dentro l'UE.[1] Dal 25 maggio 2018, il GDPR andrà a sostituire la direttiva sulla protezione dei dati (ufficialmente Direttiva 95/46/EC)[2] istituita nel 1995, abrogherà le norme del Codice per la protezione dei dati personali (dlgs.n. 196/2003) che risulteranno con esso incompatibili. Ciò potrà generare confusione per alcuni ma si attende una normativa italiana "di raccordo" che metta ordine e inserisca le norme del Codice privacy non incompatibili all'interno dell'impianto normativo del Regolamento. Con Direttiva UE 2016/680, in aggiunta a questo nuovo regolamento sarà applicata una disciplina speciale e in parte derogatrice per i trattamenti dei dati da parte dell'Autorità Giudiziaria e di tutte le forze di polizia; in ragione della caratteristica dell'istituto della direttiva europea tali trattamenti dei dati (Autorita' Giudiziaria e forze di polizia) continueranno ad essere differenti da Stato a Stato ed oggetto di una legislazione separata nazionale

[5] Le fonti principali di questo paragrafo sono le seguenti:
http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali
https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati
https://www.digital4.biz/executive/law4digital/gdpr-tutto-quello-che-avreste-voluto-sapere-ma-non-avete-osato-chiedere_436721510206.htm

Alcune novità del GDPR impongono un'attenta pianificazione fin da subito, potendo comportare modifiche organizzative significative e investimenti di natura tecnologica. Inoltre il GDPR rovescia completamente la prospettiva della disciplina di riferimento, istituendo un quadro normativo tutto incentrato sui doveri e la responsabilizzazione del Titolare del trattamento (principio di "accountability"). La nuova disciplina impone a tale soggetto di garantire il rispetto dei principi in essa contenuti, ma anche di essere in grado di comprovarlo, adottando una serie di strumenti che lo stesso GDPR indica.
In primis, il registro delle attività di trattamento, che deve contenere una serie di informazioni, tra cui le finalità del trattamento, la descrizione delle categorie di interessati e di dati personali che vengono trattati, oltre che l'indicazione delle misure di sicurezza adottate. La tenuta del registro costituisce un adempimento di fondamentale importanza nell'ottica del principio di accountability, in quanto permette di monitorare in maniera approfondita le operazioni di trattamento all'interno dell'organizzazione. Esso costituisce dunque sia uno strumento operativo di lavoro con cui censire in maniera ordinata le banche dati e gli altri elementi rilevanti per assicurare un sano "ciclo di gestione" dei dati personali, sia un vero e proprio documento di carattere probatorio mediante il quale il Titolare del trattamento può dimostrare di aver adempiuto alle prescrizioni del Regolamento.
A tal fine, può risultare utile indicare nel registro una serie di elementi non espressamente imposti dall'art. 30 del GDPR, ma comunque importanti per tener traccia delle operazioni di trattamento effettuate. Tra questi, ad esempio, la base giuridica del trattamento (ricompresa tra gli elementi che devono essere contenuti nell'informativa da consegnare all'interessato), o gli applicativi e/o database utilizzati, la cui elencazione può risultare necessaria per mappare con esattezza le misure di sicurezza implementate/da implementare, oltre che per condurre efficacemente la valutazione dei rischi.
Quest'ultima assume carattere imprescindibile per poter stabilire quali misure tecniche e organizzative adottare in azienda per garantire un livello di sicurezza appropriato al rischio stesso. La nuova normativa, infatti, abbandona il concetto di "misure minime" del Codice Privacy, sostituendolo con quello di "misure adeguate". Tale maggiore discrezionalità, tuttavia, è accompagnata, come sopra precisato, dall'onere in capo al Titolare del trattamento di poter dimostrare le ragioni che hanno portato a una determinata decisione.

Titolare del trattamento che potrà nominare un Data Protection Officer (DPO), ovvero una figura specialistica e altamente qualificata che supporti l'applicazione degli obblighi della nuova normativa, e funga da punto di contatto con le Autorità di controllo e gli interessati. La designazione del DPO è obbligatoria solo in alcuni casi (trattamenti effettuati su larga scala, posti in essere da un'Autorità pubblica/organismo pubblico, o che ricomprendono categorie particolari di dati personali). Tuttavia costituisce una buona prassi anche per le aziende che sarebbero esenti da tale adempimento.
In sostanza, l'ampio spettro di novità introdotte dal GDPR impone di definire un piano di adeguamento alla nuova normativa, coinvolgendo le diverse funzioni aziendali coinvolte in operazioni di trattamento di dati personali. È fondamentale sfruttare appieno il periodo transitorio a disposizione, per garantire la conformità alle nuove disposizioni entro il 25 maggio 2018.

LE REGOLE DA APPLICARE

Scopo

Il regolamento si applica ai dati dei residenti nell'Unione Europea. Inoltre, a differenza dell'attuale direttiva, il regolamento si applica anche a società, aziende, imprese ed enti con sede legale fuori dall'UE che trattano dati personali di residenti nell'Unione Europea. Ciò anche a prescindere dal luogo o dai luoghi ove sono collocati i server e le banche dati. Il regolamento non riguarda la gestione di dati personali per attività di sicurezza nazionale o di ordine pubblico ("le autorità competenti per gli scopi di prevenzione, indagine, individuazione e persecuzione di reati penali o esecuzione di provvedimenti penali"). Secondo la Commissione Europea "i dati personali sono qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale o pubblica. Può riguardare qualunque cosa: nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP di computer."

Responsabilità

Il principio di responsabilità legato al trattamento dei dati personali resta ancorato (come nel Codice per la protezione dei dati personali) ad un concetto di responsabilità per esercizio di attività pericolosa con una valutazione ex ante in concreto ed una sostanziale inversione dell'onere della prova. Per non rispondere del danno commesso derivante dal trattamento dei dati personali occorre sostanzialmente provare di aver fatto tutto il possibile per evitarlo. Il Regolamento aggancia e sviluppa questo tipo di responsabilità verso il concetto di Accountability (art. 5 co. 2). Occorre osservare i principi applicabili al trattamento dei dati personali di cui all'articolo 5 adempiendo alle relative obbligazioni ed essere in grado di comprovarlo.

Obblighi

I requisiti per le informative agli interessati rimangono e in parte sono ampliati. Essi devono includere il tempo di mantenimento dei dati personali e occorre fornire i contatti di chi controlla i dati e del funzionario preposto alla protezione dei dati.

È stato introdotto il diritto di contestazione delle decisioni automatizzate, compresa la profilazione (Articolo 22). I cittadini hanno ora il diritto di contestare e contrastare decisioni che hanno impatto su di loro e che sono state realizzate unicamente in base ai risultati di un algoritmo.

Tale diritto, fatta eccezione per dati personali intesi ad identificare in modo univoco una persona fisica (Articolo 9 comma 1), non si applica nel caso in cui la decisione:

- *sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;*

- *sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa inoltre misure adeguate a tutela dei diritti, della libertà e dei legittimi interessi dell'interessato;*
- *si basi sul consenso esplicito dell'interessato.*

I principi di Privacy by Design and by Default (Articolo 25) richiedono che la protezione dei dati faccia parte del progetto di sviluppo dei processi aziendali per prodotti e servizi.

Le impostazioni di privacy sono configurate su un livello alto in modo predefinito.

La risk analysis in materia di protezione dei dati personali

Le valutazioni di impatto in materia di protezione dei dati (art. 35) devono essere effettuate nei casi in cui si verifichino rischi specifici per i diritti e le libertà dei soggetti dei dati. La valutazione e la riduzione del rischio sono richieste insieme ad un'approvazione preventiva da parte delle autorità per la protezione dei dati (DPA, Data Protection Authority) per rischi elevati. I Responsabili per la protezione dei dati (Articoli 37) sono tenuti a verificare l'osservanza delle norme del Regolamento da parte dei titolari e nel caso di valutazioni di impatto, se richiesto dal titolare, sono tenuti a consultarsi con esso

Il consenso

Un valido consenso deve essere esplicitamente dato per la raccolta dei dati e per i propositi per i quali sono usati (Articolo 7; definito in Articolo 4). Pertanto se la richiesta viene inserita nell'ambito di altre dichiarazioni essa va distinta e formulata con linguaggio semplice e chiaro (Articolo 7). Condizione di validità del consenso è che le finalità per cui viene richiesto siano esplicite, legittime, adeguate e pertinenti (Articolo 5). nel caso in cui il consenso al trattamento dei

propri dati personali per una o più specifiche finalità sia stato espresso da minori esso è valido solo se il minore ha almeno 16 anni. L'età viene ridotta a 13 anni solo se lo stato membro ha previsto con legge una diversa età purché non inferiore a questa. Qualora il minore abbia un'età inferiore ai 16 o 13 anni, il consenso al trattamento deve essere dato da un genitore o da chi eserciti la potestà, e deve essere verificabile (Articolo 8). I controllori dei dati devono essere in grado di provare il consenso ("opt-in") e il consenso può essere ritirato o modificato con l'introduzione di limitazioni nel trattamento (art. 18).

La sicurezza dei dati

La sicurezza dei dati raccolti è garantita dal titolare del trattamento e dal responsabile del trattamento chiamati a mettere in atto misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio. A tal fine il titolare e il responsabile del trattamento garantiscono che chiunque faccia accesso ai dati raccolti lo faccia nel rispetto dei poteri da loro conferiti e dopo essere stato appositamente istruito, salvo che lo richieda il diritto dell'Unione o degli Stati membri (Articolo 32). A garanzia dell'interessato il Regolamento UE 2016/679 regolamenta anche il caso di trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale (Articolo 44 e ss) e prevede che l'interessato venga prontamente informato in presenza di una violazione che metta a rischio i suoi diritti e le sue libertà (Articolo 33).

Il DPO (Data Protection Officer)

Qualora l'elaborazione sia effettuata da un'autorità pubblica, fatto salvo per le corti o le autorità giudiziarie indipendenti agenti nella loro competenza giudiziaria, o qualora, nel settore privato, l'elaborazione sia effettuata da un controllore le cui attività principali consistono di operazioni di elaborazione che richiedono un monitoraggio regolare e sistematico dei soggetti dei dati, una persona esperta di legislazione e pratiche relative alla protezione dei dati deve assistere colui che li

controlla o li gestisce al fine di verificare l'osservanza interna al regolamento. Il responsabile per la protezione dei dati è una figura simile, ma non identica, al funzionario preposto all'osservanza, in quanto ci si aspetta che il primo abbia una buona padronanza dei processi informatici, della sicurezza dei dati (inclusa la gestione dei ciber-attacchi) e di altre questioni di coerenza aziendale riguardanti il mantenimento e l'elaborazione di dati personali e sensibili. Ricorda molto l'Odv (organismo di vigilanza) della legge n. 231 del 2001 sulla responsabilità penale delle persone giuridiche e il responsabile anticorruzioni per la sua autonomia, indipendenza e assenza di conflitti di interesse. L'insieme di competenze richieste si estende al di là della comprensione dell'osservanza legale di leggi e regolamenti sulla protezione dei dati e comporterà una grande preparazione e professionalità. Il monitoraggio dei Data protection office sarà onere del regolatore e non del consiglio di amministrazione dell'organizzazione che assume il funzionario. La nomina di un responsabile per la protezione dei dati all'interno di una grande organizzazione rappresenterà una sfida sia per il consiglio di amministrazione, sia per lo stesso responsabile. Considerati lo scopo e la natura della nomina, sono in gioco una miriade di questioni legate alla governance e a fattori umani che le organizzazioni e le aziende dovranno affrontare. Inoltre, chi detiene l'incarico dovrà creare un proprio team di supporto e sarà anche responsabile del proprio sviluppo professionale continuativo, dal momento che, come "mini-regolatore" ad ogni effetto, dovrà essere indipendente dall'organizzazione che lo ha assunto.

Violazioni dei dati (Data Breach – art. 33 e 34)

Il titolare del trattamento dei dati avrà l'obbligo legale di rendere note le fughe di dati all'autorità nazionale e di comunicarle entro 72 ore da quando ne è venuto a conoscenza. I resoconti delle fughe di dati non sono soggetti ad alcuno standard "*de minimis*" e debbono essere riferite all'autorità sovrintendente non appena se ne viene a conoscenza e comunque entro 72 ore. In alcune situazioni le persone di cui sono stati sottratti i dati dovranno essere avvertite.

Sanzioni

Possono essere comminate le seguenti sanzioni:

- *un'ammonizione scritta in casi di una prima mancata osservanza non intenzionale.*
- *accertamenti regolari e periodici sulla protezione dei dati*
- *una multa fino a 10 milioni di euro, o fino al 2% del volume d'affari globale registrato nell'anno precedente nei casi previsti dall'Articolo 83, Paragrafo 4 o fino a 20 milioni di euro o fino al 4% del volume d'affari nei casi previsti dai Paragrafi 5 e 6.*

Diritti degli interessati

DIRITTO ALLA CANCELLAZIONE, LIMITAZIONE E RETTIFICA

Il cosiddetto diritto all'oblio è stato sostituito da un più limitato diritto alla cancellazione nella versione del GDPR adottata dal Parlamento Europeo nel marzo del 2014. L'Articolo 17 stabilisce che il soggetto dei dati ha il diritto di richiedere la cancellazione di dati personali relativi a sé sulla base di una qualsiasi di una serie di giurisdizioni che comprendono la mancata osservanza dell'articolo 6.1 (legalità), il quale include il caso (f) in cui gli interessi o i diritti fondamentali del soggetto dei dati richiedente la loro protezione prevalgono sui legittimi interessi del controllore. L'interessato deve poter esercitare questo suo diritto con la stessa facilità con cui ha espresso il consenso al trattamento dei suoi dati. Il responsabile del trattamento, dietro richiesta dell'interessato, dovrà comunicare all'interessato i destinatari a cui ha trasmesso la sua richiesta di cancellazione (Articolo 19). Sul responsabile del trattamento grava lo stesso

onere in caso di richiesta di limitazione o di rettifica dei dati presentata dall'interessato rispettivamente ai sensi dell'art. 18 e dell'art. 16 del Regolamento UE 2016/679.

DIRITTO ALLA PORTABILITÀ

Una persona deve essere in grado di trasferire i propri dati personali da un sistema di elaborazione elettronico a un altro senza che il controllore dei dati possa impedirlo. Inoltre, i dati devono essere forniti dal controllore in un formato strutturato e di uso comune. Il diritto alla portabilità dei dati è sancito dall'Articolo 18 del GDPR. Gli esperti legali vedono nella versione finale di questa misura la creazione di un "nuovo diritto" che "si estende oltre l'ambito della portabilità dei dati tra due controllori, così come stipulato dall'Articolo 18".

LE ESIGENZE DELL'ORGANIZZAZIONE

Data l'ampiezza del perimetro di impatto del GDPR a livello aziendale, mappare il modello attuale e identificarne in modo esaustivo i gap, in relazione a quanto richiesto dal Regolamento, richiede un approccio strutturato e comprensivo di tutte le leve su cui è possibile agire in relazione all'obiettivo di adeguamento, quali:

1. **Organizzazione e ruoli**. Definizione e formalizzazione del modello organizzativo, dei ruoli e delle relative responsabilità all'interno dell'azienda, in relazione all'indirizzo e alla gestione dei temi legati alla Privacy.

2. **Persone, cultura e competenze**. Progettazione e diffusione della cultura della protezione dei dati e delle policy di sicurezza all'interno dell'organizzazione, attraverso attività di formazione e sensibilizzazione.

3. **Processi e regole**. È senza dubbio una delle aree più impattate dalle richieste di adeguamento del GDPR, basti ricordare la Privacy by design, la portabilità dei dati, la gestione dei data breach, la gestione del registro dei trattamenti, la gestione dei diritti degli interessati. Sono solo alcuni dei processi richiesti dal Regolamento che dovranno essere disegnati, implementati e presidiati nell'organizzazione.

4. **Documentazione**. Definizione delle procedure del manuale di gestione della data protection, aggiornamento dei contratti con le terze parti, adeguamento e/o stesura della documentazione di base quali informative, moduli di consenso, lettere di nomina, ecc.

5. **Tecnologia e strumenti**. Area di rilevante importanza - tipicamente anche dal punto di vista di investimenti da prevedere in ottica di piano di adeguamento - in ambito di misure di sicurezza informatica (antivirus, disaster recovery, firewall, pseudonimizzazione dati, cifratura dati, prevenzione e rilevazione data breach, Identity Management, ecc.), di sicurezza fisica (es. controllo accessi), di adozione di tool IT GRC (Governance, Risk & Compliance).

6. **Sistema di controllo**. Progettazione e gestione di un cruscotto di KPI per il monitoraggio della compliance a normative esterne (es. GDPR), regolamenti interni, progettazione di reportistica ad hoc da condividere a vari livelli dell'organizzazione.

L'OSSERVANZA DEL REGOLAMENTO NEL MODELLO ORGANIZZATIVO

Il principio di funzionamento del sistema

In relazione ai principi descritti al paragrafo precedente, il Modello Organizzativo già implementato in azienda per la prevenzione dei reati presupposto 231, si presta efficacemente per la gestione ed il monitoraggio del Regolamento Europeo oggetto della presente Parte Speciale. La flessibilità del sistema Cloudgovernance 2.0 ® ha consentito di essere in linea per i seguenti parametri:

- *Organizzazione e ruoli: l'organigramma dinamico consente, oltre a visualizzare le funzioni ed i relativi responsabili, di monitorare il rischio specifico ed implementare le necessarie azioni correttive sulla base della rilevazione delle* non conformità

- *Analisi e Gestione del Rischio: il sistema adottato nasce con lo scopo di misurare costantemente il rischio sotteso ai processi nelle attività sensibili; il Regolamento Europeo per la Protezione dei Dati Personali richiede infatti che l'azione dell'Azienda in tale ambito sia improntata ai principi di* compliance *e di* risk management *insieme; il risultato è quello di un'analisi dei rischi finalizzata al rispetto delle regole, come assicurato dalla corretta gestione delle Schede di Controllo del sistema Cloudgovernance 2.0 ®*

- *Processi e regole: le procedure aziendali vengono sottoposte ad un costante controllo, e ad una misurazione delle performances in ottica di prevenzione del rischio; anche in tal caso giova la possibilità di attribuire* non conformità *ed azioni correttive*

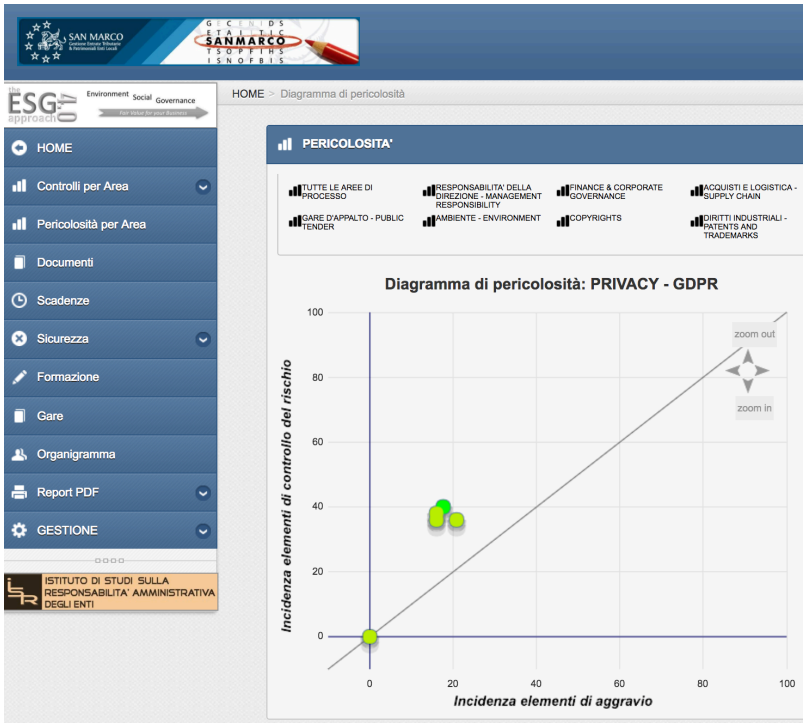
- *Documentazione: il sistema adottato presenta le caratteristiche di conservazione della documentazione necessaria, che può essere utilizzata anche a fini probatori, e collegata alle schede di controllo destinate all'analisi del rischio.*

L'applicazione delle regole e l'implementazione delle azioni di sistema

Le aree di processo e le schede di controllo già implementate per l'analisi del rischio degli altri reati presupposto sono state revisionate nella struttura, comprendendo le sanzioni indicate dalla normativa introdotta in tema di protezione dei dati personali.
Le ipotesi di sanzione misurate con lo strumento dinamico risultano quindi proporzionalmente aumentate di gravità, nella misura in cui la fase di audit abbia rilevato un pericolo di commissione dei reati presupposto che possono portare ad una condotta tipica.

All'applicazione del Regolamento Europeo è stata quindi dedicata una nuova Area di Processo, che permette di identificare le attività sensibili e valutare costantemente le necessarie azioni correttive, misurando la pericolosità delle singole funzioni interessate in organigramma, in relazione alle attività svolte.

Schermata Home del sistema Cloudgovernance 2.0 ® sull'area di processo "Privacy – GDPR"


HOME > Diagramma di pericolosità
HOME
Controlli per Area
Pericolosità per Area
Documenti
Scadenze
Sicurezza
Formazione
Gare
Organigramma
Report PDF
GESTIONE
ISTITUTO DI STUDI SULLA RESPONSABILITA' AMMINISTRATIVA DEGLI ENTI
PERICOLOSITA'
TUTTE LE AREE DI PROCESSO
RESPONSABILITA' DELLA DIREZIONE - MANAGEMENT RESPONSIBILITY
FINANCE & CORPORATE GOVERNANCE
ACQUISTI E LOGISTICA - SUPPLY CHAIN
GARE D'APPALTO - PUBLIC TENDER
AMBIENTE - ENVIRONMENT
COPYRIGHTS
DIRITTI INDUSTRIALI - PATENTS AND TRADEMARKS
Diagramma di pericolosità: PRIVACY - GDPR
zoom out
zoom in
Incidenza elementi di controllo del rischio
Incidenza elementi di aggravio
0
20
40
60
80
100

Regolamento per il funzionamento dell'Organismo di Vigilanza

Istituito ai sensi dell'art. 6 e 7 D.lgs. 231/2001

Identificazione dell'Organismo di Vigilanza

In base alle previsioni del D.Lgs. 231/01, l'organismo cui affidare il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento deve essere interno alla società (art. 6, 1° comma, lettera b) del D.Lgs. 231/01) e dotato di autonomi poteri di iniziativa e controllo.
Le Linee Guida di Confindustria, suggeriscono che si tratti di un organo diverso dal Consiglio di Amministrazione o dal Collegio Sindacale, caratterizzato da autonomia, indipendenza, professionalità e continuità di azione. Tale autonomia presuppone che l'O.d.V. riporti, nello svolgimento di questa sua funzione, solo al massimo vertice gerarchico (Direzione, ed anche Collegio Sindacale). Applicando tali principi alla realtà aziendale di SAN MARCO e in considerazione della specificità dei compiti che fanno capo all'O.d.V., sarebbe opportuno affidare il relativo incarico a due o più consulenti esterni, selezionati per le specifiche competenze tecniche e per aver partecipato alla realizzazione delle procedure organizzative e dello stesso Modello Organizzativo.
La scelta di affidare la funzione di vigilanza a tale organismo è stata privilegiata sulla base del fatto che esso è stato riconosciuto come il più adeguato ad assumere il ruolo di O.d.V., proprio per le sue caratteristiche di indipendenza, autonomia, professionalità e continuità d'azione, nonché dotato di una cultura specifica di controllo aziendale.
La nomina dell'O.d.V. così come la revoca dell'incarico affidatogli, sono atti di competenza della Direzione.

Funzione e poteri dell'Organismo di Vigilanza

All' O.d.V. è affidato il compito di vigilare:
A) sull'osservanza del Modello da parte dei Dipendenti, dei membri degli Organi Societari, dei Consulenti e dei Partner;
B) sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati;

C) sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative.
A tal fine, all'O.d.V. sono altresì affidati i seguenti compiti:

Aggiornamenti e potestà normativa:
a. emanare o sollecitare l'emanazione di disposizioni procedurali attuative dei principi e delle regole contenute nel Modello, le quali dovranno essere coerenti con le regole e le procedure aziendali già in vigore;
b. interpretare la normativa rilevante e verificare l'adeguatezza del Modello a tali prescrizioni normative, segnalando alla Direzione le possibili aree di intervento;
c. valutare le esigenze di aggiornamento del Modello, segnalando alla Direzione le possibili aree di intervento;
d. indicare al management le opportune integrazioni ai sistemi di gestione delle risorse finanziarie (sia in entrata che in uscita), già presenti in SAN MARCO , per introdurre alcuni accorgimenti idonei a rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto;
e. indicare alla Direzione l'opportunità di emanare particolari disposizioni procedurali attuative dei principi contenuti nel Modello, che potrebbero non essere coerenti con quelle in vigore attualmente nella Società, curando altresì il coordinamento delle stesse con quanto esistente.

Verifiche e controlli:
a. condurre ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura dei Processi Sensibili;
b. effettuare periodicamente verifiche mirate su determinate operazioni o specifici atti posti in essere da SAN MARCO, soprattutto nell'ambito dei Processi Sensibili, i cui risultati devono essere riassunti in un apposito rapporto da esporsi in sede di reporting agli organi societari deputati;
c. raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere trasmesse all'OdV, o tenute a sua disposizione;
d. coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il miglior monitoraggio delle attività in relazione alle procedure stabilite nel Modello.

A tal fine, l'O.d.V. ha libero accesso a tutta la documentazione aziendale che ritiene rilevante e deve essere costantemente informato dal management :

- sugli aspetti dell'attività aziendale che possono esporre SAN MARCO al rischio di commissione di uno dei Reati;
- sui rapporti con i Consulenti e Partner che operano per conto della Società nell'ambito di Operazioni Sensibili;
- sulle operazioni per le quali le procedure prevedono specifici obblighi di informativa all'O.d.V.;

e. attivare e svolgere le inchieste interne, raccordandosi di volta in volta con le funzioni aziendali interessate per acquisire ulteriori elementi di indagine.

Formazione:

a. coordinarsi con il responsabile di funzione per la definizione dei programmi di formazione per il personale stesso e del contenuto delle comunicazioni periodiche da farsi ai Dipendenti e agli Organi Societari, finalizzate a fornire agli stessi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al D.Lgs. 231/01;

b. predisporre ed aggiornare con continuità, con la collaborazione della funzione competente, il sito internet della Società contenente tutte le informazioni relative al D.Lgs. 231/01 e al Modello;

c. monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione interna necessaria al fine della sua efficace attuazione, contenente istruzioni d'uso, chiarimenti o aggiornamenti dello stesso.

Sanzioni:

•coordinarsi con la Direzione per valutare l'adozione di sanzioni disciplinari, previste dal contratto collettivo ferma restando la competenza di quest'ultima per il procedimento disciplinare e l'eventuale irrogazione della sanzione.

Linee di reporting dell'O.d.V.

Reporting dell'O.d.V. verso il vertice aziendale:

L'O.d.V. riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità, attraverso due modalità di comunicazione:

- a prima, su base continuativa, direttamente verso la Direzione;
- a seconda, su base annuale, sempre nei confronti della Direzione, al fine di commentare il rapporto predisposto dall'O.d.V. sulla attività svolta (indicando in particolare i controlli effettuati e l'esito degli stessi, le verifiche specifiche e l'esito delle stesse, l'eventuale aggiornamento della mappatura dei Processi Sensibili, ecc.) nonché, il piano dell'attività prevista per l'anno successivo.

Il reporting ha ad oggetto:

- l'attività svolta dall'ufficio dell'O.d.V.;
- le eventuali criticità (e spunti per il miglioramento) emerse sia in termini di comportamenti o eventi interni a SAN MARCO , sia in termini di efficacia del Modello.

Gli incontri con gli organi cui l'O.d.V. riferisce devono essere verbalizzati e copie dei verbali devono essere custodite dall'O.d.V. e dagli organismi di volta in volta coinvolti.
La Direzione ha la facoltà di convocare in qualsiasi momento l' O.d.V. il quale, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione del predetto organo per motivi urgenti.

Flussi informativi verso l'O.d.V.: informazioni di carattere generale ed informazioni specifiche obbligatorie

L'O.d.V. deve essere informato, mediante apposite segnalazioni da parte dei Collaboratori, degli Organi Societari e dei Terzi in generale in merito ad eventi

che potrebbero ingenerare responsabilità di SAN MARCO ai sensi del D.Lgs. 231/01.
Valgono al riguardo le seguenti prescrizioni di carattere generale:
• i Dipendenti e gli Organi Societari devono segnalare all'O.d.V. le notizie relative alla commissione, o alla ragionevole convinzione di commissione dei Reati;
• Consulenti e Partner saranno tenuti ad effettuare le segnalazioni con le modalità e nei limiti previsti contrattualmente;
• i Dipendenti avranno l'obbligo di segnalare all'O.d.V. anche le violazioni delle regole di comportamento o procedurali contenute nel presente Modello;
• le segnalazioni devono esser fatte dai Dipendenti al superiore gerarchico che provvederà a indirizzarle verso l'O.d.V. In caso di mancata canalizzazione verso l'O.d.V. da parte del superiore gerarchico o comunque nei casi in cui il Dipendente si trovi in una situazione di disagio psicologico nell'effettuare la segnalazione al superiore gerarchico, la segnalazione potrà essere fatta direttamente all'O.d.V. I Consulenti e i Partner, per quanto riguarda la loro attività svolta nei confronti di SAN MARCO , faranno la segnalazione direttamente all'O.d.V.;
• l'O.d.V. valuta le segnalazioni ricevute e adotta gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna;
• l' O.d.V. non è tenuto a prendere in considerazione le segnalazioni anonime;
• SAN MARCO garantisce i segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione e assicura in ogni caso la massima riservatezza circa l'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della società o delle persone accusate erroneamente e/o in mala fede.
Oltre alle segnalazioni relative a violazioni di carattere generale sopra descritte, gli Organi Societari, i Dipendenti e, nei modi e nei limiti previsti contrattualmente, i Consulenti e i Partner devono obbligatoriamente ed immediatamente trasmettere all'O.d.V. le informazioni concernenti:
• i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i Reati qualora tali indagini coinvolgano SAN MARCO o suoi Dipendenti od Organi Societari;

• i rapporti preparati dalle funzioni competenti nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D.Lgs. 231/01;
• le notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i Dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora essi siano legati a commissione di Reati o violazione delle regole di comportamento o procedurali del Modello.
Periodicamente l'O.d.V. propone, se del caso, alla Direzione eventuali modifiche della lista sopra indicata relativa alle informazioni obbligatorie.
L'O.d.V. ha il diritto di richiedere informazioni in merito al sistema di deleghe adottato da SAN MARCO , secondo modalità dallo stesso stabilite.

Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, report previsti nel presente Modello è conservata dall'O.d.V. in un apposito data base istituito presso il server centralizzato a disposizione di SAN MARCO .
L'accesso all'area "Sistema di Governance" di detto data base è consentito solo all'O.d.V..
Eventuali comunicazioni da e verso l'O.d.V. vengono inviate e poste all'attenzione dell'Organismo di Vigilanza mediante invio all'account di posta elettronica odv231@serit.info.

La formazione delle risorse e la diffusione del Modello

Formazione ed informazione dei Dipendenti

Ai fini dell'efficacia del presente Modello, è precipuo obiettivo di SAN MARCO quello di garantire una corretta conoscenza delle regole di condotta ivi contenute sia alle risorse già presenti in Società sia a quelle future, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nei Processi Sensibili.

La comunicazione iniziale
L'adozione del presente Modello è comunicata a tutti i Dipendenti presenti in azienda al momento dell'adozione stessa.
Ai nuovi assunti, invece, viene consegnato un set informativo (CCNL, Comunicazione adozione del Modello Organizzativo, D.Lgs. 231/01,), Procedura per la gestione delle informazioni riservate, con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza.

La formazione
L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. 231/01 è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno i destinatari funzioni di rappresentanza della società.
In particolare, SAN MARCO cura l'adozione e l'attuazione di un adeguato livello di formazione mediante idonei strumenti di diffusione e, in particolare attraverso:
- un meeting aziendale con cadenza annuale;
- il sito Internet (continuamente accessibile);
- corsi istituzionali (in aula);
- e-mail ai Dipendenti della Società.

Il sistema di informazione e formazione è supervisionato ed integrato dall'attività realizzata in questo campo dall'O.d.V. avvalendosi della collaborazione del responsabile della formazione.

Selezione ed informazione dei Consulenti e dei Partner

Relativamente ai Consulenti ed ai Partner, sentito l'O.d.V. e in collaborazione con il responsabile della gestione del personale, sono istituiti appositi sistemi in grado di orientare la selezione dei medesimi secondo criteri che tengano in debito conto i principi di prevenzione ed integrità di cui al presente Modello, principi di cui gli stessi verranno adeguatamente informati, anche con apposita clausola contrattuale che verrà inserita nei nuovi contratti.

Tutela del Whistleblower

DECRETO LEGISLATIVO 24/2023: PROTEZIONE DELLE PERSONE CHE SEGNALANO VIOLAZIONI (WHISTLEBLOWING)

Premessa. È stato pubblicato in Gazzetta Ufficiale il Decreto Legislativo 10 Marzo 2023, n. 24 "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali".

Lo scopo della direttiva è disciplinare la protezione dei whistleblowers all'interno dell'Unione, mediante norme minime di tutela, volte a uniformare le normative nazionali, a partire dal principio che coloro "che segnalano minacce o pregiudizi al pubblico interesse di cui sono venuti a sapere nell'ambito delle loro attività professionali esercitano il diritto alla libertà di espressione".

In tema di whistleblowing, il nostro Paese aveva già previsto alcune norme nel d.lgs. 20 marzo 2001, n. 165 (articolo 54-bis) e nel d.lgs. 8 giugno 2001, n. 231 (articolo 6, commi 2-bis e ss.), nonché nella legge 30 novembre 2017, n. 179.

Con il decreto legislativo approvato si abrogano le disposizioni anzidette, raccogliendo in un unico testo normativo la disciplina relativa alla tutela delle persone segnalanti.

Ambito di applicazione oggettivo e canali di segnalazione. Con riferimento alle violazioni oggetto di possibile segnalazione, va innanzitutto rilevato che il decreto legislativo comprende anche le violazioni del diritto nazionale (facoltà consentita dalla Direttiva UE), con alcune esclusioni: ad esempio, quella concernente la materia della sicurezza e difesa nazionale, così come la protezione delle informazioni classificate, del segreto professionale forense e medico e delle deliberazioni degli organi giudiziari.

L'art. 3 del decreto legislativo prevede una lista ampia di soggetti giuridici, sia del settore pubblico (art. 2, lettera p) che del settore privato (art. 2, lettera q), a cui si applica la normativa. Si tratta di una delle novità introdotte con il recepimento della direttiva.

I canali di segnalazione che il decreto legislativo prevede sono tre:

- Segnalazioni interne;
- Segnalazioni esterne;
- Divulgazioni pubbliche.

Ambito di applicazione soggettivo. Sul piano soggettivo, garantite della tutela sono le persone fisiche che operano nel contesto lavorativo del settore pubblico o privato in qualità di dipendenti o collaboratori, lavoratori subordinati e autonomi, liberi professionisti ed altre categorie specificate quali volontari e tirocinanti anche non retribuiti, gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto. La tutela delle persone segnalanti si applica anche quando il rapporto di lavoro non è stato costituito, durante il periodo di prova o dopo lo scioglimento del rapporto stesso.

Va sottolineato che le misure di protezione previste dal Capo III si applicano anche ai c.d. "facilitatori", alle persone che operano nel medesimo contesto lavorativo delle persone segnalanti, ai terzi legati da vincoli di parentela entro il sesto grado o di affinità entro il secondo grado, o legate da stabile legame affettivo con le persone segnalanti, nonché agli enti di cui le persone segnalanti sono titolari e agli enti che operano nel medesimo contesto di tali persone.

Le segnalazioni interne. Le modalità di presentazione delle segnalazioni interne sono volte a garantire la riservatezza dell'identità del segnalante.

All'art. 4 vengono indicati i soggetti, del settore privato e del settore pubblico, che necessariamente devono istituire i canali di segnalazione interna. Si tratta di una delle novità richieste dalla direttiva, che ha esteso le tutele ai whistleblowers anche del settore privato.

In particolare, per quel che concerne il settore privato, una delle novità del decreto è che dovranno predisporre i canali di segnalazione interna quei soggetti che:

- hanno impiegato, nell'ultimo anno, la media di almeno cinquanta lavoratori subordinati;
- ovvero, rientrano nell'ambito di applicazione degli atti dell'Unione di cui alle parti I.B e II dell'allegato (servizi, prodotti e mercati finanziari e prevenzione del riciclaggio o del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente), anche se nell'ultimo anno non hanno raggiunto la media di cinquanta lavoratori subordinati;
- ovvero, rientrano nell'ambito di applicazione del decreto legislativo 8 giugno 2001, n. 231, e adottano modelli di organizzazione e gestione ivi

previsti, anche se nell'ultimo anno non hanno raggiunto la media di cinquanta lavoratori subordinati.

Sul piano applicativo, il decreto legislativo stabilisce che "i Comuni diversi dai Capoluoghi di Provincia possono condividere il canale di segnalazione interna e la relativa gestione" (anche nell'ambito delle Unioni di Comuni e delle altre forme associative) e che "i soggetti del settore pubblico cui sia fatto obbligo di prevedere la figura del responsabile della prevenzione della corruzione e della trasparenza (…) affidano a quest'ultimo, anche nelle ipotesi di condivisione (…) la gestione del canale di segnalazione interna".

Per il settore privato, i soggetti che abbiano impiegato, nell'anno precedente, una media di lavoratori subordinati non superiore a 249 (il d.lgs. non prevede un limite "inferiore"), possono condividere il canale di segnalazione interna e la relativa gestione.

L'articolo 5, infine, disciplina l'iter successivo alla segnalazione.

Le segnalazioni esterne. L'articolo 6 del Decreto legislativo stabilisce le condizioni per effettuare le segnalazioni esterne, mentre l'articolo 7 indica l'ANAC quale autorità competente per tali segnalazioni, anche per il settore privato, e prevede le modalità di presentazione delle segnalazioni, attraverso canali idonei a garantire la riservatezza.

Obbligo di riservatezza e misure di protezione. Il decreto legislativo prevede norme specifiche in tema di riservatezza dell'identità delle persone che effettuano segnalazioni (art. 12 e ss. dello schema) e dedica il capo III alle misure di protezione.

Nello specifico, l'art. 17 prevede il divieto di ritorsione (con un elenco non esaustivo di casistiche al comma 4), mentre l'art. 18 individua le misure di sostegno in favore della persona segnalante.

Entrata in vigore. L'art. 24 del Decreto legislativo prevede che le disposizioni del decreto hanno effetto a decorrere dal 15 luglio 2023, con una deroga per i soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori fino a 249: per questi, infatti, l'obbligo di istituzione del canale di segnalazione interna ha effetto a decorrere dal 17 dicembre 2023.

L'iter. Nella seduta del **9 Dicembre 2022** del Consiglio dei Ministri è stato approvato, in esame preliminare, lo **schema** di Decreto Legislativo che recepisce la Direttiva UE in tema di whistleblowing.

Con questo Decreto Legislativo si raccoglie in un unico testo normativo la disciplina relativa alla tutela delle persone segnalanti, tenendo conto delle previsioni legislative vigenti e di quelle da adottare per conformarsi alla direttiva. L'iter ora prevede l'assegnazione alle seguenti Commissioni con relativi termini per l'espressione dei pareri:

- Commissioni riunite II (Giustizia) e XI (Lavoro) (Assegnato il 10 dicembre 2022 – Termine il 19 gennaio 2023)
- V Bilancio e Tesoro (Assegnato il 10 dicembre 2022 – Termine il 19 gennaio 2023)
- XIV Politiche dell'Unione Europea (Assegnato il 10 dicembre 2022 ai sensi ex art.126, co.2 – Termine il 19 gennaio 2023).

Tra le novità contenute nello schema:

- l'intervento sull'elenco di soggetti a cui si applica la protezione e i contenuti di tale tutela (es. in tema di ritorsioni sul luogo di lavoro);
- la previsione dei canali di segnalazione interna per i soggetti giuridici del settore privato superiori a 50 dipendenti, con relativa disciplina (a determinate condizioni, peraltro, sono compresi anche quelli inferiori a 50 dipendenti);
- alcune facilitazioni per i piccoli Comuni.

Nella seduta del **21** Dicembre, le Commissioni riunite II Giustizia e XI Lavoro della Camera hanno avviato l'esame dello schema di decreto legislativo. Dopo l'illustrazione dei contenuti, è stato deciso di svolgere un'attività conoscitiva con la definizione di un programma di audizioni da svolgere nella seconda settimana di gennaio.

Nella seduta del **12 Gennaio 2023**, la XIV Commissione Politiche dell'Unione Europea della Camera ha avviato l'esame dello schema di decreto: il relatore in Commissione ha annunciato la presentazione di una proposta di parere favorevole.

Le Commissioni riunite II Giustizia e XI Lavoro della Camera, nella seduta del **12 Gennaio**, hanno audito informalmente: Valentina Lostorto, Coordinatrice del Dipartimento regole e funzionamento della Pubblica Amministrazione (DIRPA) della Scuola Nazionale dell'Amministrazione; Giovanni Tartaglia Polcini, Consigliere giuridico presso il Ministero degli Affari Esteri e della Cooperazione Internazionale; Nicola Allocca, Presidente del Comitato Anticorruzione Business (BIAC), presso l'OCSE; Giorgio Fraschini, responsabile Whistleblowing presso Transparency international; Priscilla Robledo, responsabile Whistleblowing

presso The Good Lobby; rappresentanti dell'Associazione dei Componenti degli Organi di Vigilanza; rappresentanti della Federazione legali e professionisti delle amministrazioni della Repubblica (FLEPAR).
La Commissione V Bilancio della Camera, nella seduta del **18 Gennaio** ha concluso l'esame dello schema di D.lgs. sul whistleblowing esprimendo parere favorevole.
Le Commissioni riunite II Giustizia e XI Lavoro hanno proseguito l'esame nelle sedute del **17**, **18** e **19** Gennaio.
Le Commissioni riunite II Giustizia e XI Lavoro nella seduta del **25 Gennaio** hanno proseguito l'esame di una bozza di parere allo schema di decreto legislativo, convenendo di porlo in votazione nella settimana entrante.
La Commissione XIV Politiche UE approva, nella seduta del **25 Gennaio**, una proposta di **parere** favorevole allo schema.
Le Commissioni II Giustizia e XI Lavoro della Camera hanno approvato, nella seduta del **14 febbraio**, **parere** favorevole con osservazioni allo schema di decreto legislativo.
Nel frattempo, la **Commissione europea** ha deferito, in data 15 febbraio 2023, alcuni paesi, tra cui l'Italia, per il mancato recepimento e l'omessa notifica delle misure nazionali di recepimento, nei rispettivi quadri giuridici, della direttiva riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

La Tutela del Whistleblowing in San Marco Spa

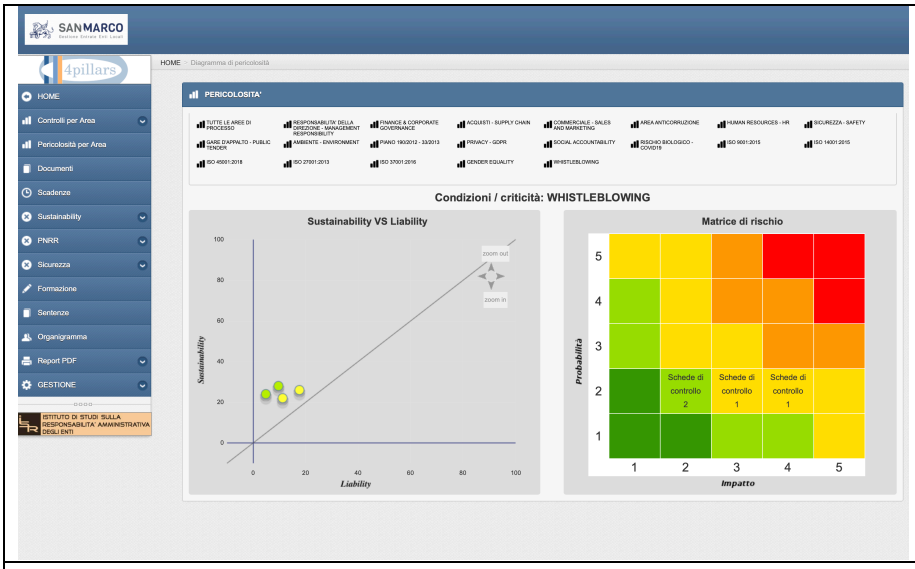
Da sempre attenta alle esigenze dei rapporti con gli Stakeholders, San Marco ha implementato fin dal 2009, con il MOG 231, una formula particolarmente avanzata di tutela del whistleblowing e di raccolta delle segnalazioni.
L'organo deputato alla raccolta delle segnalazioni è l'Organismo di Vigilanza 231, nella persona del Presidente Avvocato Pietro Domenichini, mediante email inviata all'indirizzo pietro.domenichini.vr@gmail.com e nelle modalità descritte in questo capitolo e con il supporto del sistema software 4Pillars con consente anche di effettuare una costante analisi dei rischi relativi alle attività indicate.

Modalità di controllo e analisi del rischio. Miglioramento continuo in base alle segnalazioni dei whistleblower.

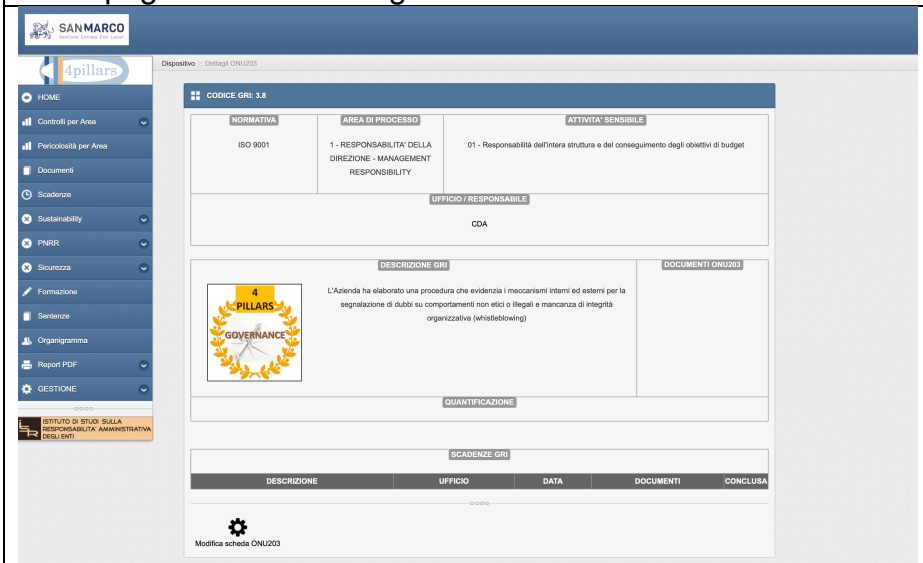
Nell'atteggiamento di San Marco Spa le segnalazioni anonime provenienti dal whistleblower non sono materia di preoccupazione o di volontà di insabbiamento o ritorsione.
Al contrario, le segnalazioni sono un importante veicolo di miglioramento continuo che ispira il funzionamento stesso dell'Azienda ed il suo rapporto con gli stakeholders.
Per questo motivo il sistema 4Pillars è stato adattato a raccogliere le segnalazioni anonime per farle diventare un motivo di azioni di miglioramento e di valutazione del comportamento e dell'organizzazione stessa dell'Azienda.

Visualizzazione delle modalità di analisi e di miglioramento continuo per il whistleblowing in San marco

Il sistema 4Pillars consente, come si diceva, di effettuare un controllo permanente e sempre aggiornato dello stato delle segnalazioni e del rischio a cui la struttura viene sottoposta.
In questi esempi possiamo visualizzare come lavora il sistema.

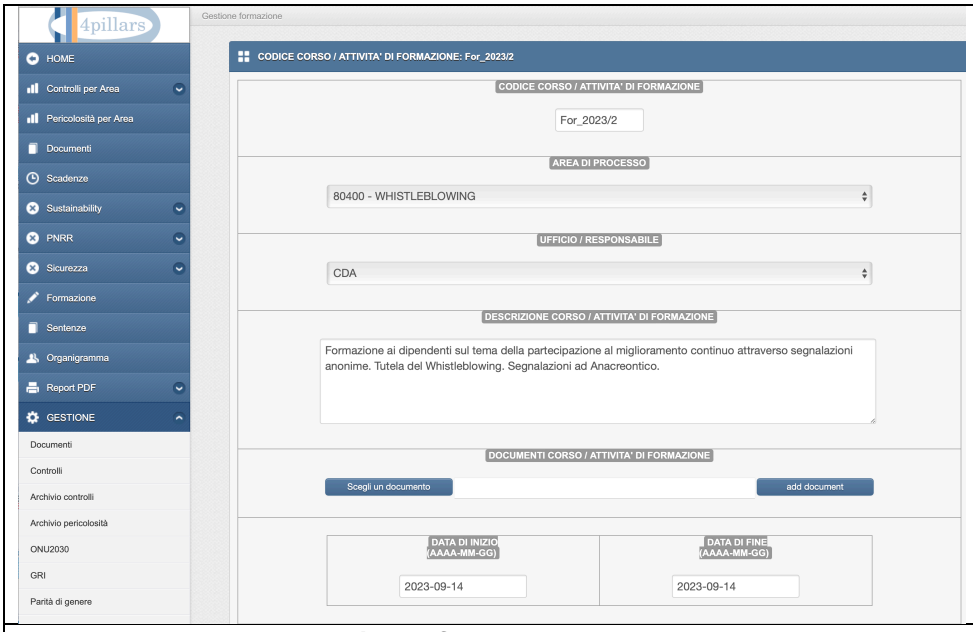


Homepage del sistema di gestione con analisi del rischio



Visualizzazione a progetto nel tema materiale della sostenibilità per quanto riguarda il whistleblowing

Scheda di controllo delle singole azioni positive a tutela del whistleblowing



Programmazione attività di formazione per settembre 2023 in materia di whistleblowing

Procedura sintetica

Il sistema di whistleblowing implementato da San Marco è a disposizione di tutti i dipendenti e delle altre parti interessate (ex dipendenti, candidati, azionisti, amministratori, fornitori, sub- fornitori e loro personale, singolarmente considerati il "***Segnalante***").
Nel più ampio contesto dei valori a cui è ispirato il nostro Codice Etico, il sistema di whistleblowing rispecchia il forte impegno di San Marco nei confronti dell'etica, della conformità e della lotta contro ogni forma di corruzione.

La presente Procedura Whistleblowing ha lo scopo di illustrare le modalità di segnalazione di illeciti e di delineare le garanzie di riservatezza e protezione a tutela dei Segnalanti.

Che tipo di condotta può essere segnalata?

In base alle leggi e ai regolamenti vigenti, possono essere segnalati diversi tipi di condotte illecite (la "***Segnalazione***"). Si può trattare di un reato, di un illecito, di una minaccia o di un danno al bene comune, di una violazione o di un tentativo di occultare una violazione di un impegno internazionale debitamente ratificato o approvato dall'Italia, di un atto unilaterale di un'organizzazione internazionale basato su tale impegno, della violazione del diritto dell'Unione europea, di leggi o regolamenti.

La denuncia può riguardare fatti accaduti o molto probabili. Il Segnalante può avere una conoscenza diretta o indiretta dei fatti.

In particolare ed a titolo esemplificativo, il sistema interno di whistleblowing di San Marco può riguardare:

- - condotte che implicano frode, corruzione, traffico di influenza illecita, riciclaggio;
- - qualsiasi caso di discriminazione o molestia morale o sessuale;
- - qualsiasi evento che comporti una violazione della normativa in materia di sicurezza sui

luoghi di lavoro, protezione, ambiente e/o qualità;

- - qualsiasi comportamento contrario al Codice Etico di San Marco o al Modello di

organizzazione e gestione di San Marco (e delle controllate interessate) o illeciti rilevanti ai sensi del Decreto Legislativo 8 giugno 2001, n. 231.

Chi riceve la segnalazione interna?

Nell'ambito della Stabile Organizzazione di San Marco, è possibile inviare la segnalazione interna *all'Organismo di Vigilanza* di San Marco Sede Secondaria ovvero, quale canale alternativo, al *Chief Corporate Officer* di San Marco Sede secondaria.

Gli organi autorizzati a ricevere le segnalazioni hanno la piena responsabilità di garantire che le stesse siano mantenute strettamente confidenziali.

Come fare una Segnalazione?

Ciascun Segnalante può inviare la propria segnalazione secondo diverse modalità. In ogni caso San Marco mette a disposizione del Segnalante una

piattaforma informatica dedicata "*San Marco Whistleblowing System*" disponibile sul sito internet di San Marco SA. L'utilizzo del canale di segnalazione informatico è caldamente consigliato al fine di poter assicurare, anche attraverso l'ausilio degli strumenti informatici, la riservatezza delle persone e dei fatti oggetto della Segnalazione.

Come vengono gestite le segnalazioni?

Al ricevimento di una Segnalazione l'organo preposto:

- - entro 72 ore lavorative (al massimo 7 giorni), invia al Segnalante un avviso di

ricezione della Segnalazione;

- - mantiene le interlocuzioni con il Segnalante e può richiedere a quest'ultimo, se

necessario, integrazioni;

- - conduce le indagini in modo tale da assicurare che le informazioni raccolte, ivi inclusa

l'identità del Segnalante, delle persone coinvolte e delle persone che assistono il Segnalante nel processo di segnalazione, siano trattate con la massima riservatezza e sicurezza;

- - fornisce riscontro alla Segnalazione entro 3 mesi dalla data dell'avviso di ricezione (della prima Segnalazione).

Segnalazioni in forma anonima

Sono possibili segnalazioni anonime. In questi casi l'organo preposto è tenuto a gestire le Segnalazioni soltanto se le stesse contengono elementi precisi e specifici nonché prove di supporto che rendano possibile dare seguito alla Segnalazione.

I Segnalanti devono agire in buona fede

L'utilizzo improprio, quindi, non in buona fede del sistema di segnalazione può esporre il suo autore a sanzioni disciplinari e/o azioni legali.

Al contrario, l'utilizzo del sistema in buona fede, anche se i fatti risultassero in seguito inesatti o non portassero ad alcun procedimento, non può esporre il Segnalante a eventuali sanzioni.

Riservatezza

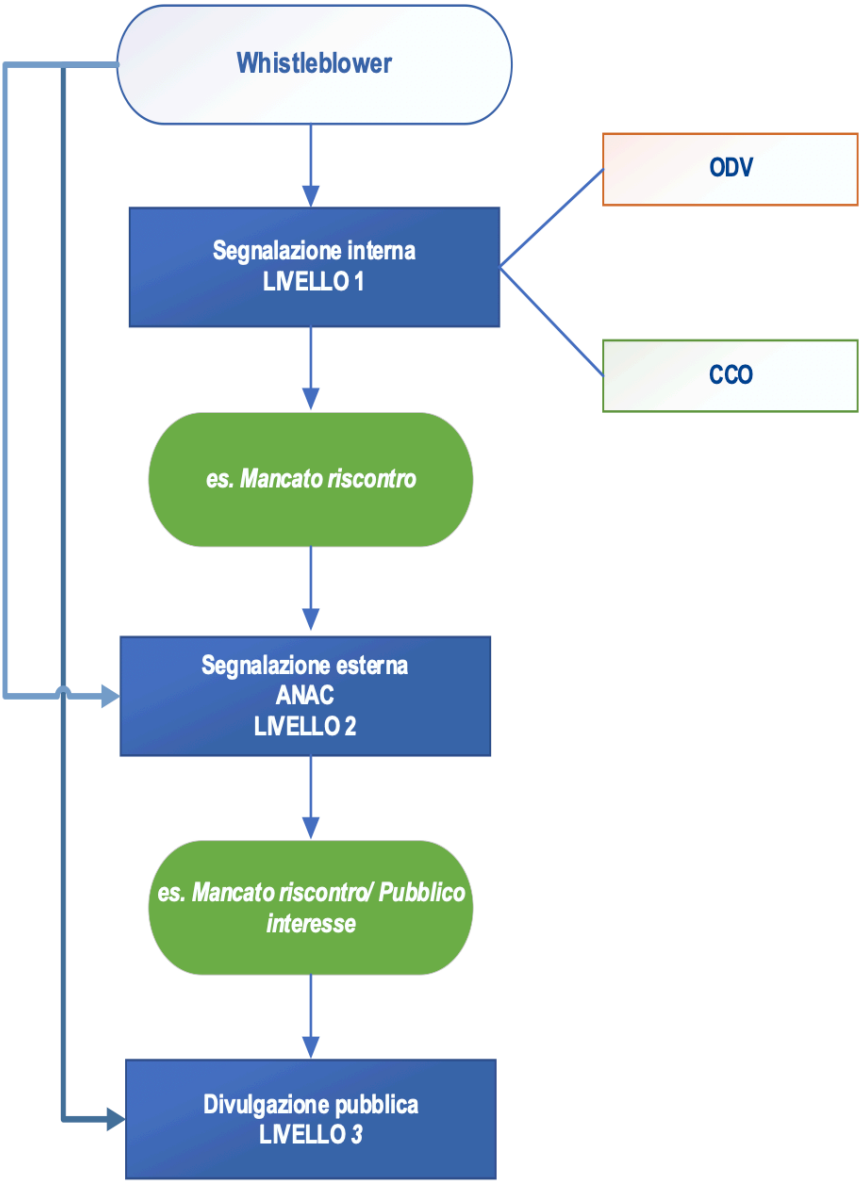
L'organo preposto svolge le indagini nella massima riservatezza. Potrà avvalersi del supporto di collaboratori interni o esterni che saranno vincolati ad accordi di riservatezza.

A meno che non sia stato dato il consenso e salvo nei casi previsti dalla legge che prevedono la comunicazione all'Autorità giudiziaria, l'identità del Segnalante, delle persone interessate e dei terzi citati nella Segnalazione sarà mantenuta riservata. Anche l'identità della persona coinvolta ed i fatti contestati saranno mantenuti riservati fino a quando l'indagine interna non si concluderà con un procedimento disciplinare e/o legale, se necessario.

Misure di protezione

San Marco garantisce che i Segnalanti che agiscono in buona fede siano protetti da ogni forma di ritorsione. San Marco non intraprenderà alcuna azione disciplinare o discriminatoria nei confronti di dipendenti che hanno fatto una Segnalazione, anche se i fatti denunciati non sono provati. Queste misure di protezione sono garantite anche ai parenti ed alle persone che hanno assistito il Segnalante nel processo di segnalazione.

Livelli di Segnalazione


Whistleblower
ODV
Segnalazione interna
LIVELLO 1
CCO
es. Mancato riscontro
Segnalazione esterna
ANAC
LIVELLO 2
es. Mancato riscontro/ Pubblico interesse
Divulgazione pubblica
LIVELLO 3

Oltre alla Segnalazione interna, il Segnalante può effettuare una segnalazione esterna (ANAC) qualora:

- - ha già effettuato una segnalazione interna e la stessa non ha ricevuto riscontro;
- - ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Il Segnalante può anche decidere di rendere di pubblico dominio le informazioni sulla Segnalazione nei casi previsti dalla legge.

Sistema disciplinare

Funzione del sistema disciplinare

La definizione di un sistema di sanzioni (commisurate alla violazione e dotate di adeguata efficacia deterrente) applicabili in caso di violazione delle regole di cui al presente Modello, rende effettiva l'azione di vigilanza dell'O.d.V. ed ha lo scopo di garantire l'efficace attuazione del Modello stesso.
La definizione di tale sistema disciplinare costituisce, infatti, ai sensi dell'art. 6, comma 1, lettera e) del D.Lgs. 231/01, un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità di SAN MARCO .
L'applicazione del sistema disciplinare e delle relative sanzioni è indipendente dallo svolgimento e dall'esito del procedimento penale che l'autorità giudiziaria abbia eventualmente avviato nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del D.Lgs. 231/01.
Il presente paragrafo contiene la descrizione delle misure sanzionatorie previste dal Contratto Collettivo Nazionale di Lavoro.

Dipendenti soggetti al CCNL

SISTEMA DISCIPLINARE

La violazione da parte dei Dipendenti soggetti al CCNL delle singole regole comportamentali di cui al presente Modello costituisce illecito disciplinare.
I provvedimenti disciplinari irrogabili nei riguardi di detti lavoratori -nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) e delle eventuali normative speciali applicabili– sono quelli previsti dall'apparato sanzionatorio dei CCNL applicati da SAN MARCO e precisamente:
- richiamo verbale;
- multa fino all'importo di 3 ore di paga ed indennità di contingenza;
- ammonizione scritta;
- sospensione dal lavoro fino a 3 giorni;
- licenziamento con preavviso;
- licenziamento senza preavviso;

Restano ferme – e si intendono qui richiamate – tutte le previsioni del richiamato CCNL, relative alle procedure ed agli obblighi da osservare nell'applicazione delle sanzioni.
Restano invariati i poteri già conferiti al management aziendale per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni.

VIOLAZIONI DEL MODELLO E RELATIVE SANZIONI

Ferma restando l'applicabilità della disciplina prevista dai sopra citati Contratti Collettivi, i comportamenti sanzionabili sono i seguenti:
1) violazione, da parte del Dipendente, di procedure interne previste o espressamente richiamate dal presente Modello (ad esempio non osservanza delle procedure prescritte, omissione di comunicazioni all'O.d.V. in merito a informazioni prescritte, omissione di controlli, ecc.) o adozione, nell'espletamento

di attività connesse ai Processi Sensibili, di comportamenti non conformi alle prescrizioni del Modello;
2) violazione di procedure interne previste dal presente Modello o adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle prescrizioni del Modello stesso che espongano la Società ad una situazione oggettiva di rischio di commissione di uno dei Reati;
3) adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle prescrizioni del presente Modello e diretti dolosamente e in modo univoco al compimento di uno o più Reati anche se poi non effettivamente commessi;
4) adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti palesemente in violazione delle prescrizioni del presente Modello, tale da determinare la concreta applicazione a carico della Società di sanzioni previste dal D.Lgs. 231/01.
Le sanzioni verranno commisurate al livello di responsabilità ed autonomia del Dipendente, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità del suo comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la Società può ragionevolmente ritenersi esposta – ai sensi e per gli effetti del D.Lgs. 231/01 – a seguito della condotta censurata.
Per quanto riguarda l'accertamento delle suddette infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni restano di competenza della Direzione. Viene previsto il necessario coinvolgimento dell'O.d.V. nella procedura di accertamento delle violazioni e di irrogazioni delle sanzioni per violazione del Modello, nel senso che non potrà essere archiviato un provvedimento disciplinare ovvero irrogata una sanzione disciplinare, per violazione del Modello, senza preventiva informazione e parere dell'O.d.V.
Il consenso all'irrogazione della sanzione non si presume, anche quando la proposta di apertura di procedimento disciplinare provenga dall'O.d.V. Ai Dipendenti verrà data un'immediata e diffusa informazione circa l'introduzione di ogni eventuale nuova disposizione, diramando una circolare interna per spiegare le ragioni che le hanno giustificate e riassumerne il contenuto.

Misure nei confronti dei dirigenti, della Direzione e dei consulenti

In caso di violazione, da parte di Dipendenti che ricoprano la qualifica di dirigenti, delle procedure previste dal presente Modello o di adozione, nell'espletamento di attività connesse con i Processi Sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso, SAN MARCO provvede ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dallo Statuto.
Al dirigente potranno anche essere revocate le procure eventualmente conferitegli.
In ogni caso delle procedure di accertamento delle violazioni e di irrogazione delle sanzioni ai dirigenti per violazione del Modello, dovrà essere preventivamente informato l'O.d.V. a cui verrà richiesto di esprimere il proprio parere.
In caso di violazione del Modello da parte della Direzione, l'O.d.V. informa l'Assemblea dei Soci i quali prendono gli opportuni provvedimenti al fine di adottare le misure più idonee previste dalla legge.
Ogni violazione da parte dei Consulenti o dei Partner delle regole di cui al presente Modello agli stessi applicabili o di commissione dei Reati è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti (cfr. Parte Speciale 1).
Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla Società, come ad esempio nel caso di applicazione alla stessa da parte dell'autorità giudiziaria delle misure previste dal D.Lgs. 231/01.
L'O.d.V. ha, come previsto dalla legge, autonomi poteri di iniziativa e controllo ai fini di vigilare sul funzionamento e l'osservanza del Modello, ma non ha poteri coercitivi o di intervento modificativi della struttura aziendale o sanzionatori nei confronti di Dipendenti, Partner o Organi Sociali, poteri questi che sono demandati ai competenti Organi Societari o funzioni aziendali, secondo i protocolli previsti nel Modello, Regolamento, Statuto.

Verifiche sull'adeguatezza del Modello

L'O.d.V. svolge continuamente attività di vigilanza sull'effettività del Modello, che si concreta nella verifica della coerenza tra i comportamenti effettivi dei destinatari ed il Modello stesso.
Inoltre l'Organismo effettua periodicamente specifiche verifiche sulla reale idoneità del Modello alla prevenzione dei Reati, anche coadiuvandosi con soggetti terzi in grado di assicurare una valutazione obiettiva dell'attività svolta.
Tale attività si può espletare in una verifica a campione dei principali atti societari e dei contratti di maggior rilevanza conclusi o negoziati dalla società in relazione ai Processi Sensibili e alla conformità degli stessi alle regole di cui al presente Modello.
Inoltre, viene svolta una review di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'O.d.V., degli eventi considerati con SAN MARCO rischiosi e della consapevolezza dei Dipendenti e degli Organi Sociali rispetto alla problematica della responsabilità penale dell'impresa con verifiche a campione.
Per le verifiche l'O.d.V. si avvale, di norma, del supporto di quelle funzioni interne o di risorse esterne che, di volta in volta, si rendano a tal fine necessarie.
Le verifiche e il loro esito sono oggetto di report annuale alla Direzione. In particolare, in caso di esito negativo, l'O.d.V. esporrà, nel piano relativo all'anno, i miglioramenti da attuare.