Modello di Organizzazione, Gestione e Controllo ai sensi del D.lgs. 231/2001 in materia di responsabilità amministrativa da reato degli enti

IDENTIFICATIVO
MM231_MOG_2.3_20241202

Versione
Ed. 2 Rev. 3 – 02/12/2024

Versione	:	Definitivo
Classificazione	:	Utilizzo Interno/Esterno

☐ : Copia soggetta ad aggiornamento

☑ : Copia non soggetta ad aggiornamento

www.maticmind.it

SOMMARIO

2 GENERALITA'

2.1 TABELLA DELLE VERSIONI

Ver.	Redazione [Funzione]	Verifica [Responsabile]	Approvazione [Responsabile]	Data emissione	Descrizione delle modifiche
1.0	Organismo di Vigilanza Maticmind	Organismo di Vigilanza Maticmind	C.d.A. Maticmind	24/01/2017	Prima emissione
2.0	G. Pavarani	Organismo di Vigilanza Maticmind	C.d.A. Maticmind	01/10/2020	Prima Revisione Adeguamento alla normativa vigente
2.1	M. Di Rienzo	Organismo di Vigilanza Maticmind	C.d.A. Maticmind	29/01/2021	Seconda revisione. Revisione del testo del documento e adeguamento Modelli Operativi
2.2	Avv. Carmine Nikita Placco	G. Pavarani Organismo di Vigilanza Maticmind	C.d.A. Maticmind	31/07/2023	Terza revisione. Revisione del testo del documento e adeguamento Modelli Operativi
2.3	Avv. Carmine Nikita Placco G. Pavarani	L. Casaccia G. Pavarani Organismo di Vigilanza Maticmind	C.d.A. Maticmind	02/12/2024	Revisione del Modello, aggiornamento normative, e allineamento all'Analisi dei Rischi

2.2 RIFERIMENTI NORMATIVI

Decreto legislativo 8 giugno 2001 n. 231

2.4 SCOPO DEL DOCUMENTO

Il presente documento illustra i principi e le regole definite del "*Modello di Organizzazione e Gestione 231*" ed ha la finalità di evitare che alla Società possa essere ascritta la responsabilità per gli illeciti amministrativi dipendenti da reati eventualmente commessi, nel suo interesse o a suo vantaggio, da soggetti posti in posizione apicale, ovvero da persone sottoposte alla loro direzione o vigilanza. Il documento è suddiviso in due sezioni: una "*Sezione Generale*" e una "*Sezione Speciale*.

2.4.1 SEZIONE GENERALE

In questa sezione del documento è presente una sintetica ricognizione dei reati presupposto applicabili e una descrizione degli obiettivi e dei destinatari del *Modello Organizzativo*. Dopo una breve illustrazione dell'avvio del progetto di adeguamento al disposto del D.Lgs. 231/2001, della storia della società, della ratio dei principi e dell'evoluzione del Decreto, sono compendiati i protocolli che compongono il *Modello Organizzativo* della Maticmind, rappresentati da:

- il sistema organizzativo
- il sistema di procure e deleghe
- il sistema di controllo della qualità, dei servizi, della sicurezza delle informazioni e della salute e sicurezza su lavoro
- le procedure di gestione
- la comunicazione ed il coinvolgimento del personale sul *Modello Organizzativo*, nonché la sua formazione ed addestramento.

2.4.2 SEZIONE SPECIALE

Questa sezione è costituita dalla descrizione di specifici ambiti, significativi ai fini della responsabilità amministrativa ex D.lgs. 231/2001, rappresentati da:

- Analisi del rischio
- modelli operativi
- *Codice Etico*
- sistema disciplinare
- Organismo di Vigilanza.

3 INTRODUZIONE

Con il Decreto Legislativo 8 giugno 2001, n. 231 recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300*" (di seguito "il Decreto"), entrato in vigore il 4 luglio 2001, il Legislatore ha adeguato la normativa italiana in materia di responsabilità delle persone giuridiche ad alcune Convenzioni Internazionali in precedenza sottoscritte dallo Stato Italiano[1].

Il Decreto, dunque, ha superato il principio secondo cui *societas delinquere non potest*[2] introducendo nell'ordinamento italiano un regime di responsabilità amministrativa (riferibile sostanzialmente alla responsabilità penale) a carico degli enti (gli enti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica, di seguito denominati "Enti") nell'ipotesi in cui alcune specifiche fattispecie di reato vengano commesse, nell'interesse oppure a vantaggio degli Enti stessi, da, come specificato all'art. 5 del Decreto:

- soggetti che rivestano funzioni di rappresentanza, amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitino, anche di fatto, la gestione e il controllo dello stesso (si tratta dei c.d. *soggetti in posizione apicale*)
- soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti di cui al pretendente punto (i c.d. *soggetti in posizione subordinata*).

Non tutti i reati commessi dai soggetti sopra indicati implicano una responsabilità amministrativa riconducibile all'Ente, atteso che sono individuate come rilevanti solo specifiche tipologie di reati.[3]

4 NORMATIVA DI RIFERIMENTO – D.LGS 231 E SUA EVOLUZIONE

Il Decreto Legislativo 8 giugno 2001, n. 231, introducendo nell'ordinamento italiano la responsabilità in sede penale degli Enti (persone giuridiche, società e associazioni anche prive di personalità giuridica), afferma il principio secondo cui gli Enti possono essere ritenuti responsabili, e conseguentemente sanzionati, in relazione a taluni reati, commessi o tentati, nell'interesse o a vantaggio dell'Ente stesso, da soggetti in posizione apicale o subordinata.

Tale responsabilità si aggiunge a quella (penale) della persona fisica che ha realizzato materialmente il reato. Quanto ai Reati societari sanzionati dal Decreto, è sufficiente che vi sia l'elemento dell'interesse, a nulla rilevando che la società abbia tratto un profitto dalla commissione dell'illecito.

[1] In particolare: Convenzione di Bruxelles, del 26 luglio 1995, sulla tutela degli interessi finanziari; Convenzione di Bruxelles, del 26 maggio 1997, sulla lotta alla corruzione di funzionari pubblici, sia della Comunità Europea che degli Stati membri; Convenzione OCSE, del 17 dicembre 1997, sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali. Come è illustrato nel prosieguo, il Legislatore ha ratificato, con la Legge n. 146/2006, la Convenzione ed i protocolli della Nazioni Unite contro il crimine organizzato transnazionale adottati dall'Assemblea Generale del 15 novembre 2000 e 31 maggio del 2001.

[2] Prima della emanazione del Decreto, era escluso che una società potesse assumere, nel processo penale, la veste di *imputato*. Si riteneva infatti, che l'art. 27 della Costituzione, che statuisce il principio della personalità della responsabilità penale, impedisse l'estensione dell'imputazione penale ad una società e, quindi, ad un soggetto" non personale". La società, dunque, poteva essere chiamata a rispondere, sotto il profilo civile, per il danno cagionato dal dipendente, ovvero, a mente degli artt. 196 e 197 cod. pen., nell'ipotesi di insolvibilità del dipendente condannato, per il pagamento della multa o della ammenda.

[3] Deve considerarsi, inoltre, che il" catalogo" dei reati presupposto rilevanti ai sensi del Decreto è in continua espansione.

Di seguito si riporta una sintetica indicazione delle categorie di reati rilevanti emerse in sede di Analisi del Rischio (Analisi del Rischio V2.2 versione 30.10.2024) condotta a tal fine - cui si rimanda per il relativo dettaglio – evidenziando da un lato la storia, ad oggi, del progressivo ampliamento del "catalogo" dei reati presupposto rilevanti ai sensi del Decreto e dall'altro l'elencazione delle sole fattispecie riferibili all'attività svolta dalla Maticmind.

La prima tipologia di reati da cui consegue la responsabilità amministrativa dell'Ente, è quella dei **reati commessi nei confronti della Pubblica Amministrazione**, che vengono dettagliati agli artt. 24 e 25 del Decreto e costituiti, per quanto applicabili alla Maticmind, da:

- frode nelle pubbliche forniture (art. 356 c.p.)
- truffa in danno dello Stato o di altro ente pubblico (art. 640, II comma, n. 1, c.p.)
- frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640-ter c.p.)
- concussione (art. 317 c.p.)
- corruzione per l'esercizio della funzione (art. 318 c.p.)
- corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)
- circostanze aggravanti (art. 319-bis c.p.)
- corruzione in atti giudiziari (art. 319-ter c.p.)
- Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)
- corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)
- pene per il corruttore (art. 321 c.p.)
- istigazione alla corruzione (art. 322 c.p.)
- peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.)
- traffico di influenze illecite (art. 346-bis c.p.)
- turbata libertà degli incanti (art. 353 c.p.)
- turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.)

Gli ulteriori artt. 314, 314-bis, 316, 316-bis, 316-ter, 640-bis c.p. ed art. 2 della L. 898 del 23 dicembre 1986 non risultano invece applicabili.

L'art. 25-bis del Decreto richiama i **reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.**

Per Maticmind assumono rilevanza le sole seguenti fattispecie:

- contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)
- introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

Non sono, invece, applicabili alla Società i reati di cui agli artt. 453, 454, 455, 457, 459, 460, 461 e 464 c.p..

Un'ulteriore e importante tipologia di reati cui è ricollegata la responsabilità amministrativa dell'Ente è, inoltre, costituita dai **reati societari**, categoria disciplinata dall'art. 25-ter del Decreto (disposizione

introdotta dal D.Lgs. 11 aprile 2002 n. 61, che individua le seguenti fattispecie, così come modificate dalla Legge 28 dicembre 2005 n. 262) e per quanto applicabili alla Maticmind:

- false comunicazioni sociali (artt. 2621 e 2621-bis c.c.)
- impedito controllo (art. 2625 cod. civ.)
- indebita restituzione di conferimenti (art. 2626 c.c.)
- illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
- operazioni in pregiudizio dei creditori (art. 2629 c.c.)
- formazione fittizia del capitale (art. 2632 c.c.)
- corruzione tra privati (art. 2635 c.c.)
- istigazione alla corruzione tra privati (art. 2635-bis c.c.)
- falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 27 D.Lgs. 27 gennaio 2010 n. 39).

Si precisa che l'art. 2623 c.c. (Falso in prospetto) - richiamato dall'art. 25-ter del Decreto - è stato abrogato dall'art. 34, comma 2, L. 28 dicembre 2005, n. 262 e la fattispecie criminosa è attualmente p.p. dall'art art.173-bis del TUF; pur in assenza di coordinamento, se ne è tenuto conto nell'Analisi del Rischio e nel Presente Modello, in via meramente cautelativa e prudenziale.
La fattispecie in argomento è stata, comunque, ritenuta irrilevante per Maticmind.

Anche l'art. 2624 c.c. (Falsità nelle relazioni o nelle comunicazioni delle società di revisione), richiamato dall'art. 25-ter del D.Lgs. n. 231/2001, è stato formalmente abrogato dall'art. 37, comma 34 del D.Lgs. 27 gennaio 2010, n. 39.
Il reato di Falsità nelle relazioni o nelle comunicazioni della società di revisione è attualmente previsto e sanzionato dall'art. 27 del D.Lgs. 27 gennaio 2010 n. 39, rubricato *Falsità nelle relazioni o nelle comunicazioni dei responsabili della revisione legale*, ma anche in questo caso non è stato effettuato il coordinamento con l'art. 25-ter del D.lgs. n. 231 del 2001: se ne è, dunque, tenuto conto nell'Analisi del Rischio e nel Presente Modello, in via meramente cautelativa e prudenziale.
La fattispecie in argomento è stata ritenuta rilevante per Maticmind.

Gli ulteriori artt. 2622, 2629-bis, 2633, 2636, 2637, 2638 c.c., 173-bis D.Lgs. n. 58/1998 e art. 54 del D.Lgs. n. 19 del 2 marzo 2023 non risultano invece applicabili.

L'intervento riformatore, con la Legge 14 gennaio 2003 n. 7, ha introdotto l'art. 25-quater, con cui si estende ulteriormente l'ambito di operatività della responsabilità amministrativa da reato ai **delitti aventi finalità di terrorismo e di eversione dell'ordine democratico** previsti dal codice penale e dalle leggi speciali.

Tali reati, dall'Analisi del Rischio condotta, non sono risultati applicabili all'Azienda.

Successivamente, la Legge 11 agosto 2003, n. 228, ha introdotto l'art. 25-quinquies, secondo il quale l'Ente è responsabile per la commissione dei **delitti contro la personalità individuale**, applicabili in ambito aziendale solo relativamente a:

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)
- pornografia minorile (art. 600-ter c.p.)

- detenzione di materiale pornografico (art. 600-quater c.p.)
- pornografia virtuale (art. 600-quater 1 c.p.) [aggiunto dall'art. 10, L. 6 febbraio 2006 n. 38].
- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.).

Gli ulteriori artt. 600-bis, 600-quinquies, 601, 602, 609-undecies c.p. non risultano invece applicabili.

Anche se Maticmind non è una società quotata, per completezza si riporta che nel 2005 la L. n. 62/2005, c.d. Legge Comunitaria e la L. n. 262/2005, meglio conosciuta come Legge sul Risparmio, hanno ancora incrementato il novero delle fattispecie di reato rilevanti ai sensi del Decreto, introducendo l'art. 25-sexies, relativo ai **reati di abuso dei mercati**, evidentemente irrilevanti per la Società.

Analogamente, anche se non applicabile alle attività aziendali, si evidenzia che, la legge 9 gennaio 2006, n. 7, ha introdotto l'art. 25-quater 1 del Decreto, che prevede la responsabilità amministrativa da reato dell'Ente nell'ipotesi che sia integrata la fattispecie di **pratiche di mutilazione degli organi genitali femminili** (art. 583-bis c.p.).

Ulteriore categoria di reati presupposto sono i c.d. **delitti di criminalità organizzata**, previsti dall'art. 24-ter del D.Lgs. n. 231/2001. I reati a tale fine applicabili in Maticmind sono:

- associazione per delinquere (art. 416 c.p.)
- associazione di tipo mafioso (art. 416-bis c.p.).

Gli ulteriori artt. 416-ter, 630, 378 c.p., 407 c.p.p., art. 291-quater del DPR 23 gennaio 1973, n. 43 e art. 74 del DPR n. 309 del 9 ottobre 1990 non risultano invece applicabili.

Il Legislatore italiano ha, ancora, integrato il Decreto mediante la Legge 3 agosto 2007 n. 123 e, in seguito, mediante il D.Lgs. 21 novembre 2007 n. 231.

Con la L. n. 123/2007 è stato introdotto l'art. 25-septies del Decreto, poi sostituito dal D.Lgs. 9 aprile 2008 n. 81, che prevede la responsabilità degli Enti per i **reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro**, con particolare riferimento a:

- omicidio colposo (art. 589 c.p.)
- lesioni personali colpose (art. 590 c.p.).

Il Dlgs. n. 231/2007, invece, ha introdotto l'art. 25-octies del Decreto, rubricato **ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita**.

I reati applicabili al contesto aziendale sono:

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

Il catalogo dei reati presupposto è stato ampliato anche attraverso la Legge 18 marzo 2008 n. 48, che ha introdotto l'art. 24-bis del Decreto, il quale estende la responsabilità degli Enti anche ad alcuni **reati c.d. informatici**, tra i quali risultano rilevanti per le attività aziendali, quelli di:

- falsità in un documento informatico pubblico avente efficacia probatoria (art. 491-bis c.p.)
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)
- danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)
- danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies c.p.)
- Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1 comma 11 D.L. 21.9.2019 n. 105, così come modificato dalla legge di conversione, L. 18.11.2019 n. 133)

Articolo 1, comma 11 del decreto-legge 21 settembre 2019 n. 105:
«11. Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni».

L'art. 640-quinquies c.p. non risulta invece applicabile.

Con la Legge n. 99 del 23 luglio 2009, è stato introdotto anche l'art. 25-bis 1, avente ad oggetto i **delitti contro l'industria e il commercio** (artt. 513, 513-bis, 514, 515, 516, 517, 517-ter, 517-quater c.p.), non applicabili all'attività aziendale.

L'art. 25-novies introduce i **delitti in materia di violazione del diritto d'autore**, tutti applicabili al contesto Maticmind (artt. 171, 171-bis, 171-ter, 171-septies e art. 171-octies L. 633/1941).

L'art. 25-decies prevede la responsabilità dell'ente per il **reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** (art. 377-bis c.p.)4, ritenuto rilevante per Maticmind.

Un'ulteriore modifica introdotta riguarda il recepimento della Direttiva 2008/99/CE del Parlamento Europeo e del Consiglio del 19 novembre 2008 sulla tutela penale dell'ambiente e della Direttiva 2009/123/CE del Parlamento Europeo e del Consiglio del 21 ottobre 2009, che modifica la Direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni.

In particolare, è stato introdotto l'art. 25-undecies dedicato ai **reati ambientali**.
Con particolare riferimento ad essi, per Maticmind sono rilevanti esclusivamente i reati di:

- attività di gestione di rifiuti non autorizzata (Art. 256 D. Lgs. 152/2006);
- traffico illecito di rifiuti (Art. 259, comma 1 D. Lgs. 152/2006);
- attività organizzate per il traffico illecito di rifiuti (Art. 260 D. Lgs. 152/2006).

Mentre le altre fattispecie di reato ivi richiamate non sono applicabili alla Società.

La modifica degli artt. 22 e 24 del Testo Unico delle leggi sull'immigrazione (D.Lgs. 286/1998), con riferimento alle sanzioni penali a carico dei datori di lavoro che impiegano manodopera immigrata priva del regolare permesso di soggiorno, crea una serie di fattispecie aggravanti alle condotte degli imprenditori che si avvalgano di lavoro nero, sanzioni che spaziano dall'ambito penale (con l'espresso richiamo al reato di sfruttamento del lavoro nero, art. 603-bis c.p.), alla presunzione della trimestralità dell'impiego al fine del computo retributivo, contributivo e fiscale; oltre alla sanzione equipollente al pagamento del costo medio di rimpatrio del lavoratore straniero assunto illegalmente, così come alla responsabilità dell'ente ex D.Lgs. 231/2001.

Con riferimento a quest'ultima, il provvedimento in esame (art. 2 del D.Lgs. 109/2012 – disposizioni sanzionatorie), introduce l'art. 25-duodecies al Decreto 231, relativo all'**impiego di cittadini di paesi terzi il cui soggiorno è irregolare**, applicabile a Maticmind, unitamente ai reati transnazionali nello stesso inseriti:

- occupazione alle proprie dipendenze di lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato (art. 22, comma 12-bis D.lgs. 286/1998);
- definizione di reato transnazionale (Art. 3 - L. 146/2006).

Non è invece applicabile a Maticmind il delitto di cui all'art. 12, comma 1, 3, 3-bis, 3-ter e comma 5, del D.Lgs. 25 luglio 1998 n. 286.

Si sottolinea infine che l'art. 23 del Decreto punisce l'inosservanza delle sanzioni interdittive che si realizza qualora all'Ente sia stata applicata, ai sensi del Decreto, una sanzione o una misura cautelare interdittiva e, nonostante ciò, lo stesso trasgredisca agli obblighi o ai divieti ad esse inerenti.

Il reato di cui all'art. 25-terdecies del D.Lgs. 231/2001, **razzismo e xenofobia**, introdotto dall'art. 5 della L. 20.11.2017 n. 167 con decorrenza dal 12.12.2017, non è rilevante per Maticmind.

Art. 5 Legge 20 novembre 2017, n. 167:

Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017.

Disposizioni per la completa attuazione della decisione quadro 2008/913/GAI sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale Caso EU Pilot 8184/15/JUST

1. Al comma 3-bis dell'articolo 3 della legge 13 ottobre 1975, n. 654, dopo le parole: «si fondano in tutto o in parte sulla negazione» sono inserite le seguenti: «, sulla minimizzazione in modo grave o sull'apologia».
2. Al decreto legislativo 8 giugno 2001, n. 231, dopo l'articolo 25-duodecies è inserito il seguente:
3. «Art. 25-terdecies (Razzismo e xenofobia). - 1. In relazione alla commissione dei delitti di cui all'articolo 3, comma 3-bis, della legge 13 ottobre 1975, n. 654, si applica all'ente la sanzione pecuniaria da duecento a ottocento quote.
4. Nei casi di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a un anno.
5. Se l'ente o una sua unità organizzativa è stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei delitti indicati nel comma 1, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'articolo 16, comma 3».

Note all'art. 5:
Il testo dell'articolo 3, della legge n. 654/1975 (Ratifica ed esecuzione della convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale, aperta alla firma a New York il 7 marzo 1966), pubblicata nella Gazzetta Ufficiale 23 dicembre 1975, n. 337, modificato dalla presente legge, così recita:
Art. 3.

1. Salvo che il fatto costituisca più grave reato, anche ai fini dell'attuazione della disposizione dell'articolo 4 della convenzione, è punito:

a) con la reclusione fino ad un anno e sei mesi o con la multa fino a 6.000 euro chi propaganda idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi;
b) con la reclusione da sei mesi a quattro anni chi, in qualsiasi modo, istiga a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi;

2. (Omissis).

3. È vietata ogni organizzazione, associazione, movimento o gruppo avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi. Chi partecipa a tali organizzazioni, associazioni, movimenti o gruppi, o presta assistenza alla loro attività, è punito, per il solo fatto della partecipazione o dell'assistenza, con la reclusione da sei mesi a quattro anni. Coloro che promuovono o dirigono tali, associazioni, movimenti o gruppi sono puniti, per ciò solo, con la reclusione da uno a sei anni.

3-bis. Si applica la pena della reclusione da due a sei anni se la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale, ratificato ai sensi della legge 12 luglio 1999, n. 232.

La categoria di reati di cui all'art. 25-quaterdecies del D.Lgs. 231/2001, **frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati**, introdotta dall'art. 5 della L. 3.5.2019 n. 39 con decorrenza dal 17.5.2019 in relazione ai reati presupposto di frode in manifestazioni sportive e di esercizio abusivo di attività di giuoco o di scommessa (artt. 1 e 4 Legge 13.12.1989 n. 401 "Interventi nel settore del giuoco e delle scommesse clandestini e tutela della correttezza nello svolgimento di manifestazioni sportive"), non è rilevante per Maticmind.

Art. 5 Legge 3.5.2019 n. 39
Reati in materia di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati:

1. dopo l'articolo 25-terdecies del decreto legislativo 8 giugno 2001, n. 231, è inserito il seguente: «Art. 25-quaterdecies (Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati). - 1. In relazione alla commissione dei reati di cui agli articoli 1 e 4 della legge 13 dicembre 1989, n. 401, si applicano all'ente le seguenti sanzioni pecuniarie:
   a) per i delitti, la sanzione pecuniaria fino a cinquecento quote;
   b) per le contravvenzioni, la sanzione pecuniaria fino a duecentosessanta quote.
2. nei casi di condanna per uno dei delitti indicati nel comma 1, lettera a), del presente articolo, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a un anno».

L. 13 dicembre 1989 n. 401
Interventi nel settore del giuoco e delle scommesse clandestini e tutela della correttezza nello svolgimento di manifestazioni sportive.

Art. 1 (Frode in competizioni sportive)

1. Chiunque offre o promette denaro o altre utilità o vantaggio a taluno dei partecipanti ad una competizione sportiva organizzata dalle federazioni riconosciute dal Comitato olimpico nazionale italiano (CONI), dall'Unione italiana per l'incremento delle razze equine (UNIRE) o da altri enti sportivi riconosciuti dallo Stato e dalle associazioni ad essi aderenti, al fine di raggiungere un risultato diverso da quello conseguente al corretto e leale svolgimento della competizione, ovvero compie altri atti fraudolenti volti al medesimo scopo, è punito con la reclusione da un mese ad un anno e con la multa da lire cinquecentomila a lire due milioni. Nei casi di lieve entità si applica la sola pena della multa.
2. Le stesse pene si applicano al partecipante alla competizione che accetta il denaro o altra utilità o vantaggio, o ne accoglie la promessa.
3. Se il risultato della competizione è influente ai fini dello svolgimento di concorsi pronostici e scommesse regolarmente esercitati, i fatti di cui ai commi 1 e 2 sono puniti con la reclusione da tre mesi a due anni e con la multa da lire cinque milioni a lire cinquanta milioni.

Art. 4 (Esercizio abusivo di attività di giuoco o di scommessa)

1. Chiunque esercita abusivamente l'organizzazione del giuoco del lotto o di scommesse o di concorsi pronostici che la legge riserva allo Stato o ad altro ente concessionario, è punito con la reclusione da sei mesi a tre anni. Alla stessa pena soggiace chi comunque organizza scommesse o concorsi pronostici su attività sportive gestite dal Comitato olimpico nazionale italiano (CONI), dalle organizzazioni da esso dipendenti o dall'Unione italiana per l'incremento delle razze equine (UNIRE).

Chiunque abusivamente esercita l'organizzazione di pubbliche scommesse su altre competizioni di persone o animali e giuochi di abilità è punito con l'arresto da tre mesi ad un anno e con l'ammenda non inferiore a lire un milione. Le stesse sanzioni si applicano a chiunque venda sul territorio nazionale, senza autorizzazione dell'Amministrazione autonoma dei monopoli di Stato, biglietti di lotterie o di analoghe manifestazioni di sorte di Stati esteri, nonché a chiunque partecipi a tali operazioni mediante la raccolta di prenotazione di giocate e l'accreditamento delle relative vincite e la promozione e la pubblicità effettuate con qualunque mezzo di diffusione.

2. Quando si tratta di concorsi, giuochi o scommesse gestiti con le modalità di cui al comma 1, e fuori dei casi di concorso in uno dei reati previsti dal medesimo, chiunque in qualsiasi modo dà pubblicità al loro esercizio è punito con l'arresto fino a tre mesi e con l'ammenda da lire centomila a lire un milione.
3. Chiunque partecipa a concorsi, giuochi, scommesse gestiti con le modalità di cui al comma 1, fuori dei casi di concorso in uno dei reati previsti dal medesimo, è punito con l'arresto fino a tre mesi o con l'ammenda da lire centomila a lire un milione.
4. Le disposizioni di cui ai commi 1 e 2 si applicano anche ai giuochi d'azzardo esercitati a mezzo degli apparecchi vietati dall'articolo 110 del regio decreto 18 giugno 1931, n. 773, come modificato dalla legge 20 maggio 1965, n. 507, e come da ultimo modificato dall'articolo 1 della legge 17 dicembre 1986, n. 9043.

4-bis. Le sanzioni di cui al presente articolo sono applicate a chiunque, privo di concessione, autorizzazione o licenza ai sensi dell'articolo 88 del testo unico delle leggi di pubblica sicurezza, approvato con regio decreto 18 giugno 1931, n. 773, e successive modificazioni, svolga in Italia qualsiasi attività organizzata al fine di accettare o raccogliere o comunque favorire l'accettazione o in qualsiasi modo la raccolta, anche per via telefonica o telematica, di scommesse di qualsiasi genere da chiunque accettati in Italia o all'estero.

4-ter. Fermi restando i poteri attribuiti al Ministero delle finanze dall'articolo 11 del decreto-legge 30 dicembre 1993, n. 557, convertito, con modificazioni, dalla legge 26 febbraio 1994, n. 133, ed in applicazione dell'articolo 3, comma 228 della legge 28 dicembre 1995, n. 549, le sanzioni di cui al presente articolo si applicano a chiunque effettui la raccolta o la prenotazione di giocate del lotto, di concorsi pronostici o di scommesse per via telefonica o telematica, ove sprovvisto di apposita autorizzazione all'uso di tali mezzi per la predetta raccolta o prenotazione.

La categoria di reati di cui all' art. 25-quinquiesdecies del Decreto, **reati tributari**, introdotta dall'art. 39 comma 2 del D.L. 26.10.2019 n. 124, con decorrenza dal 27.10.2019 ed efficacia dal 24.12.2019, così come modificato dall'allegato alla legge di conversione, L. 19.12.2019 n. 157, con decorrenza dal 25.12.2019 in relazione ai principali reati tributari previsti dal D.Lgs. 10.3.2000 n. 74, è rilevante per Maticmind.

Nello specifico, per la Società sono stati ritenuti rilevanti i seguenti reati:

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Art. 2, comma 1, del D.lgs. 10.3.2000 n. 74)
- Dichiarazione fraudolenta mediante altri artifici (art. 3 del D.Lgs. 10.3.2000 n. 74)
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, comma 1, del D.Lgs. 10.3.2000 n. 74
- Occultamento o distruzione di documenti contabili (art. 10 del D.Lgs. 10.3.2000 n. 74)
- Sottrazione fraudolenta al pagamento di imposte (art. 11 del D.Lgs. 10.3.2000 n. 74)

- Dichiarazione infedele commessa 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 (art. 4 del D.Lgs. 10.3.2000 n. 74)
- Omessa dichiarazione commessa 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 (art. 5 del D.Lgs. 10.3.2000 n. 74)
- Indebita compensazione commessa 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 (art. 10-quater del D.Lgs. 10.3.2000 n. 74)

Art. 39 D.L. 26.10.2019, n. 124
(Modifiche della disciplina penale e della responsabilità amministrativa degli enti)

1. Dopo l'articolo 25-quaterdecies del decreto legislativo 8 giugno 2001, n. 231, è aggiunto il seguente: «Art. 25-quinquiesdecies. - (Reati tributari). - 1. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'ente le seguenti sanzioni pecuniarie:
   a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, la sanzione pecuniaria fino a cinquecento quote
   b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote
   c) per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote
   d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote
   e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote
   f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote
   g) per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.

2. Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.
3. Nei casi previsti dai commi 1 e 2, si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e)». Decreto legislativo 10 marzo 2000, n. 74

Art. 2. Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.
2. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

2-bis. Se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

Art. 3. Dichiarazione fraudolenta mediante altri artifici

1. Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente: (3)
   a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;
   b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.
2. Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.
3. Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

Art. 8. Emissione di fatture o altri documenti per operazioni inesistenti

1. È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.
2. Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

2. bis. Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni.

Art. 10. Occultamento o distruzione di documenti contabili

1. Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Art. 11. Sottrazione fraudolenta al pagamento di imposte

1. È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie

altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

2. È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

Si deve tener conto dell'intervenuta approvazione del D.Lgs. 14 luglio 2020, n. 75, recante "Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la **frode che lede gli interessi finanziari dell'Unione mediante il diritto penale**", in vigore dal 30 luglio 2020 (recepimento in Italia della c.d. "Direttiva PIF"). In particolare, è stata estesa la responsabilità di società ed enti ex D.Lgs. n. 231/2001 ai seguenti reati:

- frodi IVA, qualora commesse nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a Euro 10 milioni, in ipotesi di dichiarazione infedele (art. 4, D.Lgs. n. 74/2000), omessa dichiarazione (art. 5) e indebita compensazione (art. 10-quater, D.Lgs. n. 74/2000)
- contrabbando (D.P.R. n. 43/1973), la cui sanzione è modulata a seconda che sia superata o meno la soglia di Euro 100.000
- con riferimento ai delitti contro la Pubblica Amministrazione, qualora il fatto offenda gli interessi finanziari dell'Unione europea: peculato (art. 314, comma 1, c.p., quindi con l'esclusione dell'ipotesi di uso momentaneo del bene), peculato mediante profitto dell'errore altrui (art. 316 c.p.) e abuso d'ufficio (art. 323 c.p.)
- frode nelle pubbliche forniture (art. 356 c.p.) e frode ai danni del Fondo Europeo Agricolo di Garanzia e del Fondo Europeo Agricolo per lo Sviluppo (art. 2, Legge n. 898/1986, la cui sanzione è ora aumentata in corrispondenza del superamento della soglia di Euro 100.000 di danno o profitto)
- anche a titolo di tentativo, delitti di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, D.Lgs. n. 74/2000), dichiarazione fraudolenta mediante altri artifici (art. 3) e dichiarazione infedele (art. 4).

Art. 5 D.lgs. 14 luglio 2020, n. 75
Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale (recepimento in Italia della c.d. "Direttiva PIF")

Modifiche al decreto legislativo 8 giugno 2001, n. 231

1. Al decreto legislativo 8 giugno 2001, n. 231, sono apportate le seguenti modificazioni:
   a) all'articolo 24:
      1. la rubrica è sostituita dalla seguente: «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.»
      2. al comma 1 dopo le parole: «316-ter,» è inserita la seguente «356,» e dopo le parole: «ente pubblico» sono inserite le seguenti: «o dell'Unione europea»

3. dopo il comma 2, è inserito il seguente: «2-bis. Si applicano all'ente le sanzioni previste ai commi precedenti in relazione alla commissione del delitto di cui all'articolo 2 della legge 23 dicembre 1986, n. 898.»

b) all'articolo 25:
   1. la rubrica è sostituita dalla seguente: «Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio.»
   2. al comma 1 è aggiunto, in fine, il seguente periodo: «La medesima sanzione si applica, quando il fatto offende gli interessi finanziari dell'Unione europea, in relazione alla commissione dei delitti di cui agli articoli 314, primo comma, 316 e 323 del codice penale.»

c) all'articolo 25-quinquiesdecies:
   1. dopo il comma 1 è inserito il seguente: «1-bis. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, 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, si applicano all'ente le seguenti sanzioni pecuniarie:
      a) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote
      b) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote;
      c) per il delitto di indebita compensazione previsto all'articolo 10-quater, la sanzione pecuniaria fino a quattrocento quote.»;
   2. al comma 2, le parole «al comma 1» sono sostituite dalle seguenti: «ai commi 1 e 1-bis»
   3. al comma 3, le parole «commi 1 e 2» sono sostituite dalle seguenti: «commi 1, 1-bis e 2»

dopo l'articolo 25-quinquiesdecies è aggiunto il seguente:
«Art. 25-sexiesdecies (Contrabbando). - 1. In relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, si applica all'ente la sanzione pecuniaria fino a duecento quote.

3. Quando i diritti di confine dovuti superano centomila euro si applica all'ente la sanzione pecuniaria fino a quattrocento quote.
4. Nei casi previsti dai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).».

Note all'art. 5:
Il testo dell'art. 24 del citato decreto legislativo 8 giugno 2001, n. 231, come modificato dal presente decreto, così recita:

«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.

In vigore dal 4 luglio 2001.

1. In relazione alla commissione dei delitti di cui agli articoli 316-bis, 316-ter, 356, 640, comma 2, n. 1, 640-bis e 640-ter se commesso in danno dello Stato o di altro ente pubblico o dell'Unione europea, del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.

2. Se, in seguito alla commissione dei delitti di cui al comma 1, l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità; si applica la sanzione pecuniaria da duecento a seicento quote.
2. bis. Si applicano all'ente le sanzioni previste ai commi precedenti in relazione alla commissione del delitto di cui all'art. 2 della legge 23 dicembre 1986, n. 898.
3. Nei casi previsti dai commi precedenti, si applicano le sanzioni interdittive previste dall'art. 9, comma 2 lettere c), d) ed e).».

Il testo dell'art. 25 del citato decreto legislativo 8 giugno 2001, n. 231, come modificato dal presente decreto, così recita:
«Art. 25 (Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio).

1. In relazione alla commissione dei delitti di cui agli articoli 318, 321, 322, commi primo e terzo, e 346-bis del codice penale, si applica la sanzione pecuniaria fino a duecento quote. La medesima sanzione si applica, quando il fatto offende gli interessi finanziari dell'Unione europea, in relazione alla commissione dei delitti di cui agli articoli 314, primo comma, 316 e 323 del codice penale.
2. In relazione alla commissione dei delitti di cui agli articoli 319, 319-ter, comma 1, 321, 322, commi 2 e 4, del codice penale, si applica all'ente la sanzione pecuniaria da duecento a seicento quote.
3. In relazione alla commissione dei delitti di cui agli articoli 317, 319, aggravato ai sensi dell'art. 319-bis quando dal fatto l'ente ha conseguito un profitto di rilevante entità, 319-ter, comma 2, 319-quater e 321 del codice penale, si applica all'ente la sanzione pecuniaria da trecento a ottocento quote.
4. Le sanzioni pecuniarie previste per i delitti di cui ai commi da 1 a 3, si applicano all'ente anche quando tali delitti sono stati commessi dalle persone indicate negli articoli 320 e 322-bis.
5. Nei casi di condanna per uno dei delitti indicati nei commi 2 e 3, si applicano le sanzioni interdittive previste dall'art. 9, comma 2, per una durata non inferiore a quattro anni e non superiore a sette anni, se il reato è stato commesso da uno dei soggetti di cui all'art. 5, comma 1, lettera a), e per una durata non inferiore a due anni e non superiore a quattro, se il reato è stato commesso da uno dei soggetti di cui all'art. 5, comma 1, lettera b).
5. bis. Se prima della sentenza di primo grado l'ente si è efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili ovvero per il sequestro delle somme o altre utilità trasferite e ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi, le sanzioni interdittive hanno la durata stabilita dall'art. 13, comma 2.».

Il testo dell'art. 25-quinquiesdecies del citato decreto legislativo 8 giugno 2001, n. 231, come modificato dal presente decreto, così recita:
«Art. 25-quinquiesdecies. (Reati tributari). - 1. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'ente le seguenti sanzioni pecuniarie:

a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 1, la sanzione pecuniaria fino a cinquecento quote
b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'art. 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote
c) per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'art. 3, la sanzione pecuniaria fino a cinquecento quote

d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'art. 8, comma 1, la sanzione pecuniaria fino a cinquecento quote
e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'art. 8, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote
f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'art. 10, la sanzione pecuniaria fino a quattrocento quote
g) per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'art. 11, la sanzione pecuniaria fino a quattrocento quote.

1. bis. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, 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, si applicano all'ente le seguenti sanzioni pecuniarie:
   a) per il delitto di dichiarazione infedele previsto dall'art. 4, la sanzione pecuniaria fino a trecento quote
   b) per il delitto di omessa dichiarazione previsto dall'art. 5, la sanzione pecuniaria fino a quattrocento quote
   c) c) per il delitto di indebita compensazione previsto dall'art. 10-quater, la sanzione pecuniaria fino a quattrocento quote.
2. Se, in seguito alla commissione dei delitti indicati ai commi 1 e 1-bis, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.
3. Nei casi previsti dai commi 1, 1-bis e 2, si applicano le sanzioni interdittive di cui all'art. 9, comma 2, lettere c), d) ed e).».

Direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale (recepimento in Italia della c.d. “Direttiva PIF”)
Disposizioni Generali Relative alla Frode e ad altri Reati che ledono gli Interessi Finanziari dell’Unione

Articolo 5 - Istigazione, favoreggiamento, concorso e tentativo
1. Gli Stati membri adottano le misure necessarie affinché siano punibili come reato l'istigazione, il favoreggiamento e il concorso nella commissione di uno dei reati di cui agli articoli 3 e 4.
2. Gli Stati membri adottano le misure necessarie affinché sia punibile come reato il tentativo di commettere uno dei reati di cui all'articolo 3 e all'articolo 4, paragrafo 3.

Articolo 3 - Frode che lede gli interessi finanziari dell'Unione
1. Gli Stati membri adottano le misure necessarie affinché, se commessa intenzionalmente, la frode che lede gli interessi finanziari dell'Unione costituisca reato.
2. Ai fini della presente direttiva si considerano frode che lede gli interessi finanziari dell'Unione:
   a) in materia di spese non relative agli appalti, l'azione od omissione relativa:
      i) all'utilizzo o alla presentazione di dichiarazioni o documenti falsi, inesatti o incompleti, cui consegua l'appropriazione indebita o la ritenzione illecita di fondi o beni provenienti dal bilancio dell'Unione o dai bilanci gestiti da quest'ultima, o per suo conto
      ii) alla mancata comunicazione di un'informazione in violazione di un obbligo specifico, cui consegua lo stesso effetto; ovvero

iii) alla distrazione di tali fondi o beni per fini diversi da quelli per cui erano stati inizialmente concessi

b) in materia di spese relative agli appalti, almeno allorché commessa al fine di procurare all'autore del reato o ad altri un ingiusto profitto arrecando pregiudizio agli interessi finanziari dell'Unione, l'azione od omissione relativa:

i) all'utilizzo o alla presentazione di dichiarazioni o documenti falsi, inesatti o incompleti, cui consegua l'appropriazione indebita o la ritenzione illecita di fondi o beni provenienti dal bilancio dell'Unione o dai bilanci gestiti da quest'ultima o per suo conto;

ii) alla mancata comunicazione di un'informazione in violazione di un obbligo specifico, cui consegua lo stesso effetto; ovvero

iii) alla distrazione di tali fondi o beni per fini diversi da quelli per cui erano stati inizialmente concessi, che leda gli interessi finanziari dell'Unione

c) in materia di entrate diverse dalle entrate derivanti dalle risorse proprie provenienti dall'IVA di cui alla lettera d), l'azione od omissione relativa:

i) all'utilizzo o alla presentazione di dichiarazioni o documenti falsi, inesatti o incompleti, cui consegua la diminuzione illegittima delle risorse del bilancio dell'Unione o dei bilanci gestiti da quest'ultima o per suo conto

ii) alla mancata comunicazione di un'informazione in violazione di un obbligo specifico, cui consegua lo stesso effetto, ovvero

iii) alla distrazione di un beneficio lecitamente ottenuto, cui consegua lo stesso effetto

d) in materia di entrate derivanti dalle risorse proprie provenienti dall'IVA, l'azione od omissione commessa in sistemi fraudolenti transfrontalieri in relazione:

i) all'utilizzo o alla presentazione di dichiarazioni o documenti falsi, inesatti o incompleti relativi all'IVA, cui consegua la diminuzione di risorse del bilancio dell'Unione;

ii) alla mancata comunicazione di un'informazione relativa all'IVA in violazione di un obbligo specifico, cui consegua lo stesso effetto; ovvero

iii) alla presentazione di dichiarazioni esatte relative all'IVA per dissimulare in maniera fraudolenta il mancato pagamento o la costituzione illecita di diritti a rimborsi dell'IVA.

Articolo 4 - Altri reati che ledono gli interessi finanziari dell'Unione

1. Gli Stati membri adottano le misure necessarie affinché il riciclaggio di denaro come descritto all'articolo 1, paragrafo 3, della direttiva (UE) 2015/849 e riguardante beni provenienti dai reati rientranti nell'ambito di applicazione della presente direttiva costituisca reato.
2. Gli Stati membri adottano le misure necessarie affinché, se intenzionali, la corruzione passiva e la corruzione attiva costituiscano reato.

a) Ai fini della presente direttiva, s'intende per «corruzione passiva» l'azione del funzionario pubblico che, direttamente o tramite un intermediario, solleciti o riceva vantaggi di qualsiasi natura, per sé o per un terzo, o ne accetti la promessa per compiere o per omettere un atto proprio delle sue funzioni o nell'esercizio di queste in un modo che leda o possa ledere gli interessi finanziari dell'Unione.

b) Ai fini della presente direttiva, s'intende per «corruzione attiva» l'azione di una persona che prometta, offra o procuri a un funzionario pubblico, direttamente o tramite un intermediario, un vantaggio di qualsiasi natura per il funzionario stesso o per un terzo, affinché questi compia o ometta

un atto proprio delle sue funzioni o nell'esercizio di queste in un modo che leda o possa ledere gli interessi finanziari dell'Unione.

3. Gli Stati membri adottano le misure necessarie affinché, se intenzionale, l'appropriazione indebita costituisca reato.

Con l'art. 5, comma 1, lett. d), del D.Lgs. 14 luglio 2020 n. 75, è stata introdotta la categoria di reati presupposto del **contrabbando**, *ex* art. 25-sexiesdecies del Decreto, che è stata ritenuta non applicabile a Maticmind.

Con l'art. 3, comma 1, lett. a), del D.Lgs. 8 novembre 2021 n. 184, è stata introdotta la categoria di reati presupposto **delitti in materia di strumenti di pagamento diversi dai contanti**, di cui all'art. 25-octies.1 del Decreto.
Con riferimento alla categoria in esame, per Maticmind sono state ritenute rilevanti le seguenti fattispecie:

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (Art. 493-ter c.p.);
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (Art. 493-quater c.p.)
- Frode informatica (Art. 640-ter c.p.)
- Ogni delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti.

Con l'art. 3, comma 1, della L. 9 marzo 2022 n. 22, è stata introdotta la categoria di reati presupposto dei **delitti contro il patrimonio culturale** di cui all'art. 25-septiesdecies del Decreto, ritenuta non applicabile a Maticmind.

Sempre con l'art. 3, comma 1, della L. 9 marzo 2022 n. 22, è stata introdotta anche la categoria di reati presupposto di **riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici**, *ex* art. 25-duodevicies del Decreto, ritenuta non applicabile a Maticmind.

Bisogna, infine, dare atto delle ultimissime modifiche apportate al Decreto nel corso del 2024: innanzitutto, la Legge 28.6.2024 n. 90, recante *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*, con la quale sono state in generale inasprite le pene previste per molte fattispecie, nonché modificate e/o introdotte nel catalogo 231 altre ipotesi specifiche quali, in particolare, la *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico* (art. 635-quater.1 c.p.) e il delitto di *estorsione informatica* (nuovo comma 3 dell'art 629 c.p.).

Art. 635-quater.1 c.p.
Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico).
Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa

apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329.
La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).
La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma.

Art. 629 comma 3 c.p.
Chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità.

Quindi il c.d. Decreto Carceri (D.L. 4.7.2024 n. 92 convertito, con modificazioni, dalla L. 8.8.2024 n. 112) che – nell'ambito dei reati contro la Pubblica Amministrazione – ha abrogato il delitto di abuso di ufficio *ex* art. 323 c.p. e introdotto, con il già citato art. 314-bis c.p., la fattispecie di *Indebita destinazione di denaro o cose mobili*.

Art. 314-bis
Fuori dei casi previsti dall'articolo 314, il pubblico ufficiale o l'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, li destina ad un uso diverso da quello previsto da specifiche disposizioni di legge o da atti aventi forza di legge dai quali non residuano margini di discrezionalità e intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale o ad altri un danno ingiusto, è punito con la reclusione da sei mesi a tre anni. ((La pena è della reclusione da sei mesi a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e l'ingiusto vantaggio patrimoniale o il danno ingiusto sono superiori ad euro 100.000)).

Da ultimi, la Legge 7.10.2024 n. 143 di conversione, con modificazioni, del Decreto-Legge 9.8.2024 n. 113, recante *misure urgenti di carattere fiscale, proroghe di termini normativi ed interventi di carattere economico*, c.d. Decreto Omnibus, che – con riguardo specifico ai delitti in materia di violazione del diritto d'autore, ma non solo – introduce, a carico di soggetti qualificati partitamente individuati, un obbligo di segnalazione di condotte, compiute o tentate, penalmente rilevanti ai sensi della stessa legge sul diritto d'autore o dell'art.615-ter c.p (Accesso abusivo a un sistema informatico o telematico) o dell'art.640-ter c.p. (Frode informatica) e la conseguente nuova fattispecie di omissione dell'obbligo stesso (art. 174-sexies della L. 633/1941).

Alla finalità di maggior contrasto della pirateria online, si accompagnano nella norma l'ulteriore obbligo, per gli stessi soggetti, di designare e notificare all'Autorità per le garanzie nelle comunicazioni un punto di contatto che consenta loro di comunicare direttamente, per via elettronica, con l'Autorità medesima ai fini dell'esecuzione del dettato normativo, nonché – e, soprattutto, nell'economia del presente documento – il richiamo finale all'applicazione dell'art. 24-bis del Decreto 231/2001 sui Reati informatici e di trattamento illecito di dati.

Art. 174-sexies

1. I prestatori di servizi di accesso alla rete, i soggetti gestori di motori di ricerca e i fornitori di servizi della società dell'informazione, ivi inclusi i fornitori e gli intermediari di Virtual Private Network (VPN) o comunque di soluzioni tecniche che ostacolano l'identificazione dell'indirizzo IP di origine, gli operatori di content delivery network, i fornitori di servizi di sicurezza internet e di DNS distribuiti, che si pongono tra i visitatori di un sito e gli hosting provider che agiscono come reverse proxy server per siti web, quando vengono a conoscenza che siano in corso o che siano state compiute o tentate condotte penalmente rilevanti ai sensi della presente legge, dell'articolo 615-ter o dell'articolo 640-ter del codice penale, devono segnalare immediatamente all'autorità giudiziaria o alla polizia giudiziaria tali circostanze, fornendo tutte le informazioni disponibili.

2. I soggetti di cui al comma 1 devono designare e notificare all'Autorità per le garanzie nelle comunicazioni un punto di contatto che consenta loro di comunicare direttamente, per via elettronica, con l'Autorità medesima ai fini dell'esecuzione della presente legge. I soggetti di cui al comma 1 che non sono stabiliti nell'Unione europea e che offrono servizi in Italia devono designare per iscritto, notificando all'Autorità il nome, l'indirizzo postale e l'indirizzo di posta elettronica, una persona fisica o giuridica che funga da rappresentante legale in Italia e consenta di comunicare direttamente, per via elettronica, con l'Autorità medesima ai fini dell'esecuzione della presente legge.

3. Fuori dei casi di concorso nel reato, le omissioni della segnalazione di cui al comma 1 e della comunicazione di cui al comma 2 sono punite con la reclusione fino ad un anno. Si applica l'articolo 24-bis del decreto legislativo 8 giugno 2001, n. 231.

E, infine, il Decreto-Legge 11.10.2024 n. 145, recante *Disposizioni urgenti in materia di ingresso in Italia di lavoratori stranieri, di tutela e assistenza alle vittime di caporalato, di gestione dei flussi migratori e di protezione internazionale, nonché dei relativi procedimenti giurisdizionali*, che ha modificato l'art. 22 D.Lgs n.286/1998 sul lavoro subordinato a tempo determinato e indeterminato e, conseguentemente, l'art. 25-duodecies inerente all'impiego di cittadini di paesi terzi il cui soggiorno è irregolare – peraltro, senza particolare incidenza ai fini del presente Modello – con finalità di ulteriore prevenzione e contrasto dell'immigrazione irregolare, nonché di maggior tutela delle vittime di intermediazione illecita e sfruttamento del lavoro (con rimodulazione specifica degli indici di sfruttamento di cui all'art 603-bis c.p.).

5 LE SANZIONI PREVISTE DAL DECRETO

Secondo il dettato del Decreto e come accennato nell'introduzione, l'Ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- da "persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente 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" (c.d. soggetti in posizione apicale, art. 5, comma 1, lett. a) del Decreto)
- da persone sottoposte alla direzione o alla vigilanza di soggetti in posizione apicale (c.d. soggetti sottoposti all'altrui direzione, art. 5, comma 1, lett. b) del Decreto).

Per espressa previsione legislativa (art. 5, comma 2 del Decreto) l'Ente non risponde se le persone indicate hanno agito nell'interesse esclusivo proprio o di terzi.

Nell'ipotesi in cui i soggetti di cui all'art. 5 del Decreto commettano uno dei reati previsti dagli artt. 24 e ss. dello stesso, l'Ente può subire, a mente dell'art. 9 del Decreto, l'irrogazione delle seguenti sanzioni:

a) sanzioni pecuniarie
b) sanzioni interdittive
c) confisca
d) pubblicazione della sentenza.

Dal punto di vista generale, è opportuno precisare che l'accertamento della responsabilità dell'Ente, nonché la determinazione *dell'an* e del *quantum* della sanzione, sono attributi al Giudice penale competente per il procedimento relativo ai reati dai quali dipende la responsabilità amministrativa.

L'Ente è ritenuto responsabile dei reati individuati dagli artt. 24 e ss. (ad eccezione delle fattispecie di cui all'art. 25 *septies* e dalle leggi speciali che hanno integrato il Decreto) anche se questi siano stati realizzati nelle forme del tentativo. In tali casi, però, le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà.

Ai sensi dell'art. 26 del Decreto l'Ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento.

a) Sanzioni pecuniarie

Le sanzioni pecuniarie trovano regolamentazione negli artt. 10, 11 e 12 del Decreto e si applicano in tutti i casi in cui sia riconosciuta la responsabilità dell'Ente. Le sanzioni pecuniarie vengono applicate per ''quote'', in numero non inferiore a 100 e non superiore a mille.

Il Giudice determina il numero di quote sulla base degli indici individuati dal I comma dell'art. 11, ovvero tenendo conto della gravità del fatto, del grado della responsabilità dell'Ente nonché dell'attività svolta per eliminare od attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti, mentre l'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente coinvolto allo scopo di assicurare l'efficacia della sanzione (art. 11 del Decreto).

b) Sanzioni interdittive

Le sanzioni interdittive, individuate dal comma II dell'art. 9 del Decreto ed irrogabili nelle sole ipotesi tassativamente previste e solo per alcuni reati, sono:

- l'interdizione dall'esercizio dell'attività
- la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito
- 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 e servizi.

Inoltre, le sanzioni interdittive sono applicate solo se ricorre almeno una delle seguenti condizioni:

1. l'Ente ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso:
   - da soggetti in posizione apicale, ovvero
   - da soggetti sottoposti all'altrui direzione e vigilanza quando la commissione del reato è stata determinata o agevolata da gravi carenze organizzative
2. in caso di reiterazione degli illeciti.

   Come per le sanzioni pecuniarie, il tipo e la durata delle sanzioni interdittive sono determinati dal Giudice tenendo conto della gravità del fatto, del grado di responsabilità dell'Ente e dell'attività svolta dall'Ente per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti (I comma dell'art. 11). In ogni caso, le sanzioni interdittive hanno una durata minima di tre mesi e massima di due anni.

   In luogo dell'applicazione della sanzione, il giudice può disporre la prosecuzione dell'attività dell'Ente da parte di un commissario giudiziale.
   Inoltre, le sanzioni interdittive possono essere applicate all'Ente sia all'esito del giudizio e, quindi, accertata la colpevolezza dello stesso, sia in via cautelare (art. 45), ovvero quando:
   - sono presenti gravi indizi per ritenere la sussistenza della responsabilità dell'Ente per un illecito amministrativo dipendente da reato
   - emergono fondati e specifici elementi che facciano ritenere l'esistenza del concreto pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede

   Anche in tale ipotesi, in luogo della misura cautelare interdittiva, il giudice può nominare un commissario giudiziale.

   Come misura cautelare, può essere disposto anche il sequestro del prezzo e/o del profitto del reato.
   Le sanzioni dell'interdizione dell'esercizio dell'attività, del divieto di contrarre con la P.A. e del divieto di pubblicizzare beni o servizi possono essere applicate – nei casi più gravi – in via definitiva.

   L'inosservanza delle sanzioni interdittive costituisce un reato autonomo previsto dal Decreto come fonte di possibile responsabilità amministrativa dell'Ente (art. 23).

c) Confisca

La confisca del prezzo o del profitto del reato è una sanzione obbligatoria che consegue alla eventuale sentenza di condanna (art. 19).

La confisca del prezzo o del profitto del reato può essere prevista anche per equivalente e quindi avere ad oggetto anche beni o altre utilità di valore equivalente.

La pubblicazione della sentenza è una sanzione eventuale e presuppone l'applicazione di una sanzione interdittiva (art. 18).

Poiché la responsabilità amministrativa della persona giuridica si aggiunge a quella (penale) della persona fisica che ha materialmente commesso il reato, entrambe le sanzioni sono oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale.

L'accertamento della responsabilità dell'Ente, attribuito al giudice penale, avviene mediante:

- la verifica della sussistenza del reato presupposto per la responsabilità dell'Ente
- l'accertamento in ordine alla sussistenza dell'interesse o vantaggio dell'Ente alla commissione del reato da parte del suo dipendente o apicale
- il sindacato di idoneità sul Modello di Organizzazione e Gestione.

Il sindacato del giudice circa l'astratta idoneità del *Modello Organizzativo* a prevenire i reati di cui al Decreto è condotto secondo il criterio della c.d. "prognosi postuma". Il giudizio di idoneità è, cioè, formulato secondo un criterio sostanzialmente ex-ante, per cui il giudice si colloca, idealmente, nella realtà aziendale nel momento in cui si è verificato l'illecito per saggiare la congruenza del modello adottato.

d) Pubblicazione della sentenza

All'esito del processo segue una sentenza:

- di esclusione della responsabilità dell'ente (se l'illecito non sussiste od è insufficiente o contraddittoria la prova)
- di condanna (con applicazione della sanzione pecuniaria e/o interdittiva).

Presso il Casellario Giudiziale Centrale è istituita l'Anagrafe Nazionale delle Sanzioni Amministrative presso cui sono iscritte le sentenze e/o i decreti divenuti irrevocabili.

Per completezza, infine, deve osservarsi che l'Autorità Giudiziaria può, altresì, a mente del Decreto, disporre:

- il sequestro preventivo delle cose di cui è consentita la confisca (art. 53)
- il sequestro conservativo dei beni mobili e immobili dell'Ente qualora sia riscontrata la fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento della sanzione pecuniaria, delle spese del procedimento o di altre somme dovute allo Stato (art. 54).

6 ADOZIONE E ATTUAZIONE DI UN MODELLO DI ORGANIZZAZIONE E GESTIONE QUALE ESIMENTE DELLA RESPONSABILITÀ

Il Legislatore riconosce, agli artt. 6 e 7 del Decreto, forme specifiche di esonero della responsabilità amministrativa dell'Ente.

In particolare, l'art. 6, comma I, prescrive che, nell'ipotesi in cui i fatti di reato siano ascrivibili a soggetti in posizione apicale, l'Ente non è ritenuto responsabile se prova che:

a) ha adottato ed attuato, prima della commissione del fatto, un Modello di Organizzazione e Gestione (di seguito "*Modello Organizzativo*") idoneo a prevenire reati della specie di quello verificatosi;
b) ha nominato un organismo, indipendente e dotato di autonomi poteri di iniziativa e di controllo, con l'incarico di vigilare sul funzionamento, efficacia, adeguatezza ed osservanza del *Modello Organizzativo*, nonché di curane l'aggiornamento (di seguito "Organismo di Vigilanza" o "OdV");
c) il reato è stato commesso eludendo fraudolentemente le misure previste dal *Modello Organizzativo*;
d) non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza di cui alla precedente lettera b).

Nel caso dei soggetti in posizione subordinata, l'adozione e l'efficace attuazione del *Modello Organizzativo* importa che l'Ente è chiamato a rispondere solo nell'ipotesi in cui il reato sia stato reso possibile dall'inosservanza degli obblighi di direzione e vigilanza (combinato di cui ai commi I e II dell'art. 7).

I successivi commi III e IV introducono due principi che appaiono rilevanti e decisivi ai fini dell'esonero della responsabilità dell'Ente per entrambe le ipotesi di reato ascrivibili a soggetti in posizione apicale (art. 5, lett. a) e a soggetti in posizione subordinata (art. 5, lett. b).

In particolare, è previsto che:

- il *Modello Organizzativo* preveda misure idonee sia a garantire lo svolgimento dell'attività nel rispetto della legge, sia a scoprire tempestivamente situazioni di rischio, tenendo in considerazione il tipo di attività svolta nonché la natura e la dimensione dell'organizzazione
- l'efficace attuazione del *Modello Organizzativo* richiede una verifica periodica e la modifica dello stesso qualora siano scoperte significative violazioni delle prescrizioni di legge o qualora intervengano significativi mutamenti nell'organizzazione o normativi; condizione essenziale di efficacia è, altresì, l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure organizzative (art. 6, comma II, lett. e).

7 L'IDONEITA' DEL MODELLO ORGANIZZATIVO

Affinché il *Modello Organizzativo* possa essere valutato idoneo, in linea anche con le interpretazioni della giurisprudenza, si ritiene che il *Modello Organizzativo* debba:

1. essere adottato partendo da una c.d. "mappatura" dei rischi di reato specifica ed esaustiva e non meramente descrittiva o ripetitiva del dato normativo
2. prevedere che i componenti dell'Organo di Vigilanza posseggano capacità specifiche in relazione ai compiti affidati
3. prevedere quale causa di ineleggibilità a componente dell'Organo di Vigilanza la sentenza di condanna (o di patteggiamento) anche non irrevocabile
4. differenziare tra formazione rivolta ai dipendenti nella loro generalità, ai dipendenti che operano in specifiche aree di rischio ed ai preposti al controllo interno
5. prevedere corsi di formazione, loro frequenza, obbligatorietà della partecipazione, controlli di frequenza e di qualità sul contenuto dei programmi
6. prevedere espressamente la comminazione di sanzioni disciplinari nei confronti dell'Organo Amministrativo, direttori generali che per negligenza ovvero imperizia non abbiano saputo individuare, e conseguentemente eliminare, violazioni del *Modello Organizzativo* e, nei casi più gravi, la perpetrazione di reati
7. prevedere sistematiche procedure di ricerca e identificazione dei rischi quando sussistano circostanze particolari (es. emersione di precedenti violazioni, elevato turn-over del personale)
8. prevedere periodicamente sia controlli di routine che controlli a sorpresa nei confronti delle attività aziendali sensibili
9. prevedere e disciplinare l'obbligo per i dipendenti, i direttori, l'Organo Amministrativo delle società di riferire all'Organo di Vigilanza notizie rilevanti e relative alla vita dell'Ente, a violazioni del *Modello Organizzativo* o alla consumazione di reati. In particolare, deve fornire concrete indicazioni sulle modalità attraverso le quali coloro che vengono a conoscenza di comportamenti illeciti possono riferire all'Organo di Vigilanza
10. contenere protocolli specifici e concreti.

8 LINEE GUIDA ELABORATE DALLE ASSOCIAZIONI DI CATEGORIA

In base a quanto previsto dal comma III dell'art. 6 del Decreto, i Modelli di Organizzazione, Gestione e Controllo possono essere adottati sulla base dei codici di comportamento (es. Linee Guida) redatti dalle Associazioni di categoria rappresentative degli Enti, approvati dal Ministero di Giustizia tramite la procedura prevista dal Decreto.

La prima Associazione a redigere un documento di indirizzo per la costruzione dei Modelli di Gestione ex D.Lgs. n. 231/2001 è stata Confindustria (Associazione di riferimento della Maticmind) che, nel marzo del 2002, ha emanato delle Linee Guida, poi parzialmente modificate e aggiornate varie volte, di cui le ultime prima nel marzo 2014 e poi nel giugno 2021 [5].

In particolare, la prima versione delle Linee Guida è stata elaborata nel 2002 dal Gruppo di lavoro sulla "Responsabilità amministrativa delle persone giuridiche", costituito nell'ambito del Nucleo Affari Legali, Finanza e Diritto d'Impresa di Confindustria.

Il primo aggiornamento, sulla base anche dei rilievi sollevati dal Ministero, aveva riguardato, in particolare, l'ambito delle aree a rischio reato, i protocolli preventivi e l'Organismo di Vigilanza. Ulteriori aggiustamenti erano stati apportati in considerazione delle prime esperienze applicative realizzate dalle associazioni e dalle imprese, nonché delle novità intervenute sugli assetti interni delle società di capitali per effetto della riforma del diritto societario.

A seguito dei numerosi interventi legislativi che, nel frattempo, hanno modificato la disciplina sulla responsabilità amministrativa degli enti, estendendone l'ambito applicativo a ulteriori fattispecie di reato, il Gruppo di lavoro di Confindustria ha provveduto ad aggiornare le Linee Guida per la costruzione dei modelli organizzativi. Nel febbraio 2008 la versione aggiornata delle Linee Guida è stata trasmessa al Ministero della Giustizia.

L'adeguamento delle Linee Guida, che ha riguardato sia la parte generale che l'appendice relativa ai singoli reati (c.d. case study), è diretto a fornire indicazioni in merito alle misure idonee a prevenire la commissione dei nuovi reati-presupposto. Si tratta, in particolare, dei reati di: abusi di mercato, pedopornografia virtuale, pratiche di mutilazione degli organi genitali femminili, criminalità organizzata transnazionale, omicidio colposo e lesioni personali colpose gravi o gravissime commessi con violazione delle norme sulla salute e sicurezza sul lavoro, riciclaggio. Con specifico riferimento agli abusi di mercato, l'adeguamento è stato realizzato a seguito di un approfondito confronto con la Consob.

Il 2 aprile 2008 il Ministero della Giustizia ha comunicato la conclusione del procedimento di esame della nuova versione delle Linee Guida di Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo. Le Linee Guida sono state approvate in quanto l'aggiornamento è stato ritenuto "complessivamente adeguato e idoneo al raggiungimento dello scopo fissato dall'art. 6, comma 3 del D. Lgs. n. 231/2001".

[5] Tutte le versioni delle Linee Guida di Confindustria sono state poi giudicate adeguate dal Ministero di Giustizia (con riferimento alle Linee Guida del 2002, cfr. la "Nota del Ministero della Giustizia" del 4 dicembre 2003 e, con riferimento agli aggiornamenti del 2014 e del 2021, cfr. la "Nota del Ministero della Giustizia" del 21 luglio 2014 e la "Nota del Ministero della Giustizia" dell'8 giugno 2021).

Il Ministero ha inoltre ricordato che la piena efficacia delle Linee Guida lascia impregiudicata ogni valutazione sulle modalità della loro implementazione e sulla concreta attuazione dei modelli di organizzazione e gestione da parte dei singoli enti, affiliati o meno all'Associazione.

Quindi, nel marzo 2014, all'esito di un ampio e approfondito lavoro di riesame, Confindustria ha completato i lavori di aggiornamento delle Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D.Lgs. n. 231/2001.

La nuova versione adegua il precedente testo del 2008 alle novità legislative, giurisprudenziali e della prassi applicativa nel frattempo intervenute, mantenendo la distinzione tra le due Parti, generale e speciale.
In particolare, le principali modifiche e integrazioni della Parte generale riguardano: il nuovo capitolo sui lineamenti della responsabilità da reato e la tabella di sintesi dei reati presupposto; il sistema disciplinare e i meccanismi sanzionatori; l'organismo di vigilanza, con particolare riferimento alla sua composizione; il fenomeno dei gruppi di imprese.

La Parte speciale, dedicata all'approfondimento dei reati presupposto attraverso appositi "case study", è stata oggetto di una consistente rivisitazione, volta non soltanto a trattare le nuove fattispecie di reato presupposto, ma anche a introdurre un metodo di analisi schematico e di più facile fruibilità per gli operatori interessati.

Come previsto dallo stesso D. Lgs. n.231/2001 (art. 6, co. 3), il documento è stato sottoposto al vaglio del Ministero della Giustizia che il 21 luglio 2014 ne ha comunicato l'approvazione definitiva.

Un ulteriore aggiornamento è, infine, quello del giugno 2021, che arriva decorsi 7 anni.

La versione ultima tiene conto dei nuovi reati presupposto inseriti a Catalogo 231 e dedica particolare spazio al sistema integrato di gestione dei rischi nonché a quello di segnalazione delle violazioni interne (cd. whistleblowing).

In sintesi, le Linee Guida di Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo forniscono alle associazioni e alle imprese indicazioni di tipo metodologico su come predisporre un *Modello Organizzativo* idoneo a prevenire la commissione dei reati indicati nel decreto, consentendo all'ente l'esonero dalla responsabilità e dalle relative sanzioni (pecuniarie e interdittive).

La Linee Guida di Confindustria costituiscono, pertanto, l'imprescindibile punto di partenza per la corretta costruzione del *Modello Organizzativo*, benché le indicazioni in esse fornite richiedono un successivo adattamento da parte delle imprese. Ogni *Modello Organizzativo*, infatti, per poter esercitare la propria efficacia preventiva, va costruito tenendo presenti le caratteristiche proprie dell'impresa cui si applica. Il rischio reato di ogni impresa è strettamente dipendente dal settore economico, dalla complessità organizzativa - non solo dimensionale - dell'impresa e dell'area geografica in cui essa opera.

9 IL MODELLO DI ORGANIZZAZIONE E GESTIONE DI MATICMIND

9.1 MATICMIND

Da molti anni Maticmind S.p.A. opera con successo nel settore dell'Information & Communication Technology in qualità di System Integrator ad alta specializzazione. La capacità di definire e integrare soluzioni sulla base delle esigenze dei propri Clienti rende la società un partner innovativo ed affidabile.

Maticmind in uno scenario in continua e frenetica evoluzione negli ultimi anni ha lavorato molto per innovare il proprio portafoglio di offerta. Alla fine del 2015 ha concluso due operazioni straordinarie di acquisizione. La prima ha visto l'ingresso in Maticmind di oltre 150 profili professionali operanti a vario titolo nell'ambito delle metodologie e dello sviluppo applicativo, provenienti dalla multinazionale americana HP Enterprise. Tale operazione le ha permesso di inaugurare un proprio Competence Center applicativo focalizzato sui servizi di consulenza, sviluppo, test e manutenzione di software applicativo. La seconda ha portato sempre nel 2015 all'acquisizione di Tecnonet, un system integrator attivo sul territorio italiano con oltre 200 addetti.

Nel corso del biennio 2016-2018 Maticmind ha ampliato ulteriormente il suo portafoglio di offerta concludendo alcune acquisizioni nel campo della Sicurezza delle Informazioni (Managed Security Services e servizi di consulenza), acquisendo la società Business-e facente parte del gruppo ITWay.

L'allargamento delle partecipazioni ha portato, negli ultimissimi anni, a far sì che del Gruppo facciano oggi parte integrante, tra le altre, le controllate SIO S.p.A., Sind S.p.A., Recrytera S.r.l., Page Europa S.r.l. ed EngiNe S.r.l..

Maticmind con oltre 900 dipendenti di cui più di 400 professionisti certificati assicura in questo modo una presenza capillare e radicata sul territorio italiano che le consente di affermarsi come partner tecnologico a livello nazionale grazie anche ad importanti partnership con leader di mercato nel settore ICT.

L'azienda ha ottenuto le certificazioni ISO9001:2015 (Sistemi di Qualità), ISO20000:2018 (Sistemi di Service Management), ISO27000:2013, (Sistemi di Sicurezza delle Informazioni) e ISO45000:2018 (ispirata alla OHSAS18000 relativa alla Salute e Sicurezza sul Lavoro); ISO14001 ed ISO14064-1, certificazioni ambientali e di rendicontazione dei gas serra, ed opera perciò in conformità alle norme UNI EN ISO di riferimento per le seguenti attività:

"*progettazione di sistemi e soluzioni per Telecomunicazioni, e commercializzazione, installazione, assistenza e manutenzione di apparati e reti per Telecomunicazioni. Erogazione di servizi di Network Operation Center (NOC), Security Operation Center (SOC), Vulnerability Assessment e Penetration Test e di servizi helpdesk nella gestione e risoluzione di problematiche nel campo delle telecomunicazioni e della sicurezza delle informazioni. Progettazione, sviluppo e manutenzione di software per applicazioni e sistemi informativi. Servizi di consulenza IT e reingegnerizzazione dei processi aziendali.*"

Nel corso dell'ultimo anno al Società ha inoltre acquisito le certificazioni PDR125, ISO37001, ISO27017 ed ISO27018 oltre ad aver esteso il campo delle operazioni ISO9001 alla IAF28.

9.1.1 AMBITO DI COMPETENZA

Lo scenario di riferimento di Maticmind è quello di garantire soluzioni integrate di connettività, Security, Data Center, Virtualizzazione, Voce, Video e Cloud arrivando a soluzioni sempre più orientate alle applicazioni e ai servizi a valore aggiunto, assicurando una profonda interazione tra le piattaforme infrastrutturali e quelle applicative.

Attraverso la partnership con i maggiori Vendor mondiali Maticmind ha acquisito un ruolo predominante come partner tecnologico per le più importanti realtà italiane impegnate nella trasformazione delle proprie infrastrutture (operatori di telecomunicazioni, aziende, pubblica amministrazione centrale e locale), posizionandosi saldamente ai vertici del mercato della System Integration.

Il mercato di riferimento di Maticmind comprende settori strategici quali il Finance, il Government, l'Enterprise e il Service Provider, potendo vantare più di 1500 Clienti nel mercato italiano e referenze di assoluto valore sia in termini di clientela che di progetti realizzati.

Maticmind è inoltre uno dei pochi System Integrator in Italia in grado di mettere a disposizione dei propri Clienti un Solution Center dove poter mostrare le più recenti architetture e tecnologie integrate (Cisco, Dell Technologies, VMware, Citrix, Infovista, Checkpoint, Fortinet, F5, Forcepoint, Cloud4Wi, Nuage, Splunk, Kaltura e molte altre).

9.1.2 DISTRIBUZIONE TERRITORIALE

La seguente tabella riporta le sedi operative Maticmind e le attività in esse svolte.

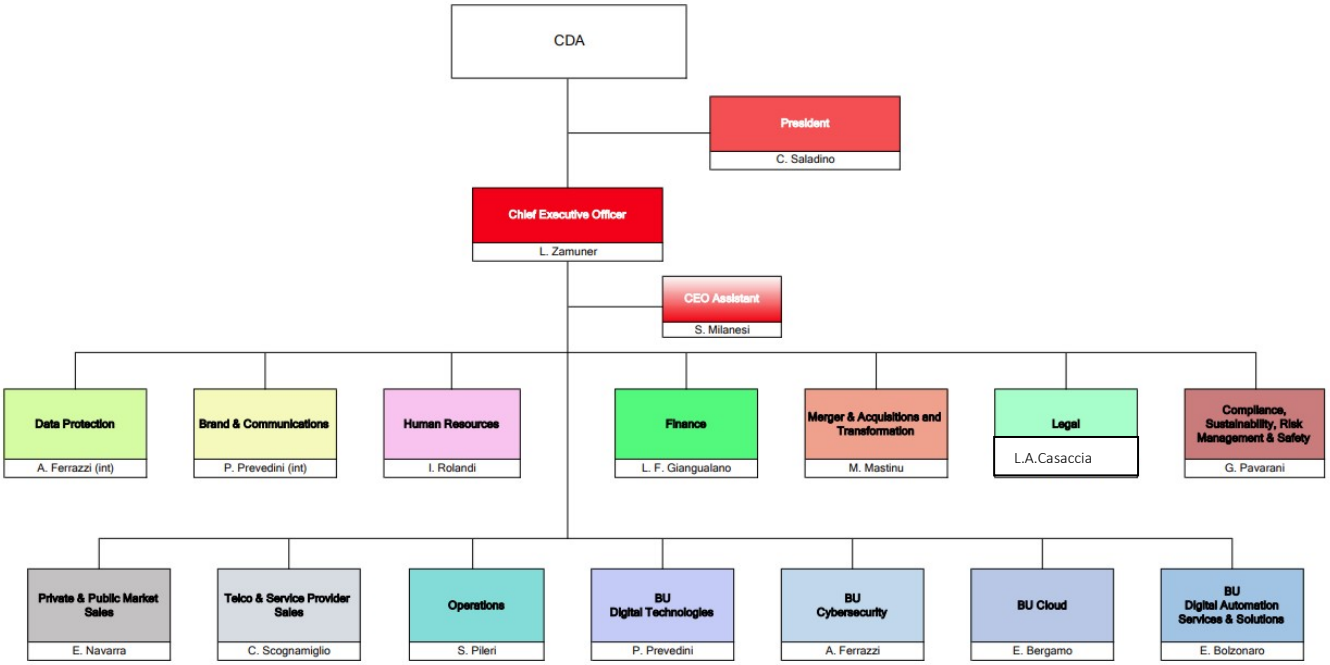
Sedi Maticmind								
Città	Indirizzo	Attività						
		Dir	Comm	Tecn	Log	Amm	NOC	SOC
Torino (TO)	c.so Unione Sovietica 612/15c			✓			✓	
Milano (M)	Via R. Bracco, 6	✓	✓	✓		✓		
Padova (PD)	Galleria Spagna 28		✓	✓			✓	
Modena (MO)	via Magellano 1		✓	✓	✓	✓		
Sesto Fiorentino (FI)	via Avogadro 34		✓	✓				
Roma (RM)	via Carucci 131	✓	✓	✓		✓	✓	✓
Ciampino (RM)	Via A. Segni 18/20				✓			
Napoli (NA)	Via Lauria D4		✓	✓		✓		
Modugno (Bari)	Via degli Orafi n.12		✓	✓				
San Giovanni La Punta (CT)	via Cristoforo Colombo 13		✓	✓				
Palermo	ViaTrapani,1D		✓	✓				

Legenda :

Dir	Direzione
Comm	Comerciale
Tecn	Tecnica
Log	Logistica
Amm	Amministrativa
NOC	Network Operation Center
SOC	Security Operation Center

9.1.3 ORGANIZZAZIONE E PRINCIPALI ATTIVITA'

Il sistema organizzativo della Maticmind è interamente strutturato in modo da assicurare alla Società l'attuazione delle strategie e il raggiungimento degli obiettivi. La struttura della Maticmind, infatti, è stata creata tenendo conto della necessità di dotare la Società di una organizzazione tale da garantirle la massima efficienza ed efficacia operativa.



Il modello organizzativo si basa essenzialmente sulla definizione di:

- tre Business Unit focalizzate sui principali ambiti tecnologici indirizzati dalla società: digital technologies, cybersecurity e IOT;
- due Direzioni Commerciali trasversali sull'offerta, che indirizzano verticalmente i mercati;
- una Direzione Operations unico che garantisce la gestione e il delivery dei progetti e l'erogazione dei servizi;
- strutture di Staff a supporto delle attività operative.

Tale modello ha l'obiettivo, da un lato, di assicurare il presidio tecnologico e di mercato, sia favorendo l'evoluzione del portfolio di offerta in linea con i principali trend del settore ICT e le esigenze dei clienti sia agevolando l'integrazione con le offerte delle altre aziende del Gruppo, dall'altro, di garantire maggiore efficienza ed efficacia nell'esecuzione dei servizi professionali e nell'implementazione delle soluzioni.

Al fine di perseguire tali obiettivi, Maticmind assume la seguente organizzazione.

- BUSINESS UNIT Digital Technologies, con l'obiettivo di garantire il presidio tecnologico e lo sviluppo della proposizione negli ambiti networks, digital workplace, IT infrastructure, cloud e application;

- **BU Cybersecurity**, con l'obiettivo di garantire il presidio tecnologico e lo sviluppo della proposizione nell'ambito della sicurezza informatica e cybersecurity

- BU Digital Application Services & Solutions con l'obiettivo di garantire il presidio tecnologico e lo sviluppo della proposizione nell'ambito delle soluzioni IOT, Smart Building, Smart Metering e Digital Twin;

DIREZIONI COMMERCIALI

- **Private & Public Market** con l'obiettivo di massimizzare il focus sulle specifiche esigenze dei clienti e posizionare in modo più efficace la Value Proposition aziendale attraverso un approccio verticale ai mercati privato e pubblico.
- **Telco & Service Provider** con l'obiettivo di seguire in maniera accurata e puntuale il mercato dei Telco Operatore e dei Service Provider, nell'ottica di incrementare il focus sulle specifiche esigenze dei clienti.

Direzione Operation: è trasversale alle Business Units, assicura efficacia ed efficienza nella conduzione ed esecuzione dei progetti e nella fornitura dei servizi ai clienti. La funzione ha quindi il compito di garantire il delivery di applicazioni, progetti (networks, IT infrastructure, digital workplace e cybersecurity) e l'erogazione dei servizi gestiti nel rispetto dei tempi, della qualità e dei costi attesi, puntando sulle competenze distintive e sulla decisa automazione dei processi, eseguire il monitoraggio, il controllo e la sincronizzazione dei benestare che consentano la trasformazione del backlog in fatturato, l'accertamento dei ricavi e dei costi delle commesse, utilizzare e sviluppare tutte le leve disponibili, tra le quali l'information technology e i processi di acquisto competitivi, per ottimizzare i costi.

Cloud Business Unit, con l'obiettivo di Supportare Maticmind alla commercializzazione delle soluzioni ed i servizi relativi alle tecnologie cloud, supportare Maticmind nello spazio delle soluzioni Data & AI afferenti a servizi cloud native, Identificare e proporre soluzioni legate a tool e piattaforme software inerenti alla gestione, l'ottimizzazione, l'automazione del mondo cloud, ivi incluse le piattaforme middleware a Microservizi, sviluppare il portfolio di servizi gestiti nell'ambito della cloud Operation, favorendone l'istituzione e il posizionamento sul mercato, garantire supporto mirato e puntuale alla forza commerciale nella proposizione, favorire le sinergie con le altre aziende del gruppo negli ambiti di offerta indicati

Brand & Communications: con l'obiettivo di guidare la comunicazione interna ed esterna, attraverso iniziative legate alla presenza digitale, alla partecipazione ad eventi e alla pubblicazione su testate nazionali e riviste di settore al fine di massimizzare il riconoscimento sul mercato del brand aziendale.

Human Resources: con l'obiettivo di gestire il personale, garantendo l'applicazione di politiche di valorizzazione e retention, guidare il processo di selezione e inserimento di nuovi talenti, attraverso politiche di attrazione di professionisti riconosciuti dal mercato e consolidamento di relazioni con università, istituti. governare il processo di Payroll, garantire la corretta applicazione delle normative in tema di risorse umane.

Finance, con l'obiettivo di presidiare la redazione di documenti contabili di bilancio, controllare i flussi finanziari, verifica la corretta allocazione delle risorse economiche e finanziarie, seguire le operazioni di

budget, contabilità generale e contabilità analitica e industriale. La funzione supporta e coordina le attività per le società del Gruppo nel conseguimento di analoghi obiettivi.

M&A e Transformation con l'obiettivo di guidare l'intero processo di merger and acquisition di possibili aziende target in linea con le strategie di crescita inorganica di Gruppo e definire priorità del piano di trasformazione del Gruppo.

Legal, con l'obiettivo di supportare le funzioni aziendali, con particolare attenzione alle Direzioni Commerciali, nella gestione degli aspetti legali e normativi che emergono nella conduzione delle attività di business.

Direzione Compliance, Sustainability, Risk Management & Safety, con l'obiettivo di assicurare la piena osservanza della normativa riguardante l'attività svolta e le relazioni con le Parti Interessate (Stakeholder) e dunque garantire una piena e continua conformità agli standard e alle normative vigenti, definire e sviluppare per Maticmind i piani ESG e CSR (Corporate Social Responsibility). La funzione supporta le società del Gruppo nel conseguimento di analoghi obiettivi.

La struttura organizzativa messa in campo da Maticmind S.p.A. per soddisfare al meglio le proprie esigenze di business prevede **nello specifico** una Direzione Vendite, che ha compito di stabilire il rapporto con i Clienti dal punto di vista commerciale ed una Direzione Operation, che a sua volta si suddivide in ulteriori strutture finalizzate a:

- supportare la Direzione Vendite
- svolgere le attività tecnico operative finalizzate all'erogazione di prodotti e/o servizi.

9.1.3.1 DIREZIONE VENDITE

La Direzione Vendite è organizzata in tre Direzioni Commerciali focalizzate rispettivamente sui mercati Corporate, Government e Telco & SP.

La **Direzione Vendite Area Mercato** propone ai propri Clienti le soluzioni del portfolio aziendale in modo diretto, al fine di assicurare un focus specifico sul mercato oppure tramite la vendita indiretta attuando accordi di collaborazione con operatori di telecomunicazioni.

Indirizza inoltre le soluzioni aziendali alla risoluzione di problematiche legate all'IT e alle telecomunicazioni degli enti centrali e locali della Pubblica Amministrazione, con un approccio ai Clienti diretto o indiretto (tramite operatore di telecomunicazioni). L'organizzazione è ulteriormente articolata sul territorio con le strutture focalizzate a soddisfare le esigenze ICT prevedendo specifiche strutture atte a garantire la copertura dell'intero territorio nazionale:

- Nord Ovest
- Nord Est
- Centro
- Sud.

La Direzione Vendite Vendite Telco è focalizzata sulle esigenze tecnologiche ed i servizi degli operatori di telecomunicazioni. Le azioni commerciali in questo settore merceologico sono condotte sia direttamente

da Maticmind con la propria struttura di vendita che tramite collaborazioni commerciali con Partner italiani e stranieri.

9.1.3.2 DIREZIONE OPERATION

La *Direzione Operation* assicura il corretto svolgimento delle attività operative, siano esse servizi professionali o servizi gestiti mettendo in campo le competenze tecnologiche dei propri professionisti determinate in base alle esigenze del mercato di riferimento. L'organizzazione della *Direzione Operation* è strutturata in tre macro funzioni:

- Project Management Office (PMO) che include la struttura di governo dei progetti (project management) e La Logistica integrata;
- Application & Technologies con il compito di espandere i servizi relativo alle applicazioni software e competence center;
- Infrastructure con il compito di rilasciare i servizi tecnici di installazione e manutenzione;
- Managed servces;
- ICT
- Procurement
- Safety& facility

Nei Competence Center si concentrano e si sviluppano le competenze specialistiche per ogni ambito tecnologico che compone l'offerta Maticmind. Ogni Competence Center:

- garantisce supporto alla forza vendite mediante attività di advisory tecnologica e progettazione tecnica
- sostiene l'innovazione di prossimità per le tecnologie di competenza
- fornisce supporto specialistico e attività progettuali
- assicura la qualità dei servizi erogati.

Per la *Progettazione delle Offerte* sono impiegate le strutture di:

- Technical Advisory
- Solution Engineering

La struttura di *Technical Advisory* garantisce supporto alla forza vendite mediante attività di advisory tecnologica e progettazione tecnica avanzata per l'impiego di nuove tecnologie o architetture evolute. Sostiene inoltre l'innovazione di prossimità mediante scouting tecnologico e benchmarking, restituendo al Cliente un punto di vista costantemente aggiornato per i contesti tecnologici di competenza.

La struttura di *Solution Engineering* è responsabile della fattibilità, della qualificazione tecnica dell'opportunità e della finalizzazione dell'Offerta tecnico-economica (e relativi allegati tecnici). In fase propositiva la struttura di *Solution Engineering* supporta la Direzione Vendite nella proposta commerciale mediante l'impiego dei suoi specialisti per tutte le tecnologie a portafoglio.

Entrambe le strutture sono coinvolte nel design delle architetture proposte e nella costruzione del modello di servizio a seconda del livello di complessità richiesto.

Per l'*Implementazione e la Realizzazione dei Progetti* e delle attività contrattualizzate sono impiegate le strutture di:

- Consultant

- Delivery & Operation

La struttura dei *Consultant* è impiegata su progetti particolarmente complessi od innovativi dove è necessario un approccio di tipo consulenziale e si compone di figure con competenze di eccellenza trasversali rispetto alla tecnologia adottata.

La struttura di *Delivery & Operation* è responsabile delle attività tecniche ed implementative di dispositivi, reti, accessori e schemi funzionali di collegamento/connessione realizzate presso le sedi del Cliente, corredate da eventuali piani operativi, nel rispetto delle normative e degli standard vigenti (ad esempio Salute e Sicurezza sul Lavoro).

Per la *Qualità dei Servizi Erogati* sono impiegate le strutture di:

- Assurance
- Managed Services

Le strutture di *Assurance* e di *Managed Services* (*Network Operation Center – NOC* e *Security Operation Center – SOC*) sono responsabili dell'analisi dell'*Incident* notificato e del coordinamento delle attività atte alla rimozione delle cause di eventuali guasti hardware o malfunzionamenti software sull'infrastruttura oggetto di assistenza, con l'obiettivo finale di ripristinare le funzionalità nel più breve tempo possibile secondo i Livelli di Servizio contrattualizzati. Si occupano inoltre di servizi di monitoraggio e di gestione operativa delle configurazioni, generando opportuna allarmistica al superamento di specifiche soglie o al verificarsi di particolari eventi.

Entrambe le strutture sono attivate sulla base delle segnalazioni gestite dal *Customer Care* Maticmind e sono composte da professionisti soggetti a formazione continua in modo da poter acquisire le conoscenze necessarie per gestire il maggior numero di tecnologie possibili e ridurre i tempi di analisi relativi alle problematiche indicate dai Clienti, fornendo così soluzioni immediate. In casi particolari possono avvalersi di un supporto di secondo e terzo livello grazie a tutte le professionalità che operano all'interno del *Competence Center*.

9.1.4 LA MISSION AZIENDALE

Maticmind considera la propria reputazione (individuale e collettiva) il più importante patrimonio aziendale: pone quindi particolare attenzione a tutte le "Parti Interessate" (Dipendenti, Clienti, Fornitori, etc.) che contribuiscono a far crescere l'azienda.

Ritiene essenziale esprimere con chiarezza e condividere principi, valori, regole e responsabilità comuni che ne orientano i comportamenti nelle relazioni con il mercato, con le comunità in cui opera, con le persone che vi collaborano e con chi ha un legittimo interesse nei confronti delle attività svolte, a cui sono soggetti tutti coloro i quali operano nel contesto aziendale.

Nell'esercizio della propria attività imprenditoriale Maticmind assume come principi ispiratori il rispetto delle norme inderogabili di legge e di contratto nonché del proprio *Codice Etico*, espressione di sintesi delle norme interne e delle normative dei paesi in cui opera, in un quadro di legalità, correttezza, trasparenza, riservatezza e rispetto della dignità della persona.

Maticmind, al fine di assicurare sempre più condizioni di trasparenza e correttezza nella conduzione degli affari delle attività aziendali, ha inoltre ritenuto adottare il presente "*Modello di Organizzazione e Gestione*" in linea con le prescrizioni del Decreto.

Maticmind ritiene che l'adozione del presente *Modello Organizzativo*, unitamente alla contemporanea emanazione del *Codice Etico* e del Codice Disciplinare, costituisca, al di là delle prescrizioni di legge, un ulteriore valido strumento di sensibilizzazione di tutti i dipendenti e di tutti coloro che collaborano con Maticmind, al fine di far seguire, nell'espletamento delle proprie attività, comportamenti corretti e trasparenti in linea con i valori etico-sociali cui si ispira Maticmind nel perseguimento del proprio oggetto sociale, e tali comunque da prevenire il rischio di commissione dei reati contemplati dal Decreto.

Ai fini della predisposizione del presente *Modello Organizzativo*, Maticmind ha proceduto all'analisi delle proprie aree di rischio tenendo conto delle prescrizioni del Decreto e delle Linee Guida formulate da Confindustria.

In attuazione di quanto previsto dal Decreto, l'Organo Amministrativo di Maticmind ha approvato il presente *Modello Organizzativo* comprensivo del *Codice Etico* e del Codice Disciplinare e in attuazione del medesimo ha contemporaneamente costituito l'Organismo di Vigilanza, con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del *Modello Organizzativo* stesso, nonché di curarne l'aggiornamento nei termini e nei modi previsti dal presente *Modello Organizzativo*.

Come sancito dal Decreto, il *Modello Organizzativo* è un "atto di emanazione dell'Organo Dirigente".

Nell'eventualità in cui si rendesse necessario procedere all'implementazione del *Modello Organizzativo* per ulteriori e/o nuove fattispecie di reato previste nel Decreto ritenute meritevoli di attenzione da parte della dirigenza di Maticmind, anche in relazione ai pareri che saranno espressi dall'Organismo di Vigilanza, è demandato all'Organo Amministrativo di Maticmind il potere di integrare il presente *Modello Organizzativo* in una fase successiva, mediante apposita delibera.

Allo stato, Maticmind ha proceduto all'implementazione del presente *Modello Organizzativo* con riferimento ai reati previsti ad oggi dal D.Lgs. 231/2001.

Tutta la gestione del *Modello di Organizzazione e Gestione* è supportata dal *Sistema di Gestione Integrato* che comprende il sistema documentale riguardante le certificazioni ottenute relative alle norme standard UNI EN ISO.

9.2 FINALITA' DEL MODELLO ORGANIZZATIVO

La legge prevede l'adozione del Modello di Organizzazione e Gestione in termini di facoltatività e non di obbligatorietà, tuttavia la mancata adozione del *Modello Organizzativo* espone l'ente alla responsabilità per gli illeciti realizzati da amministratori e dipendenti.

Inoltre, prescindendo dall'aspetto strettamente giuridico-sanzionatorio, l'adozione di un sistema di regole volte a ribadire la compliance dell'impresa non solo rispetto a norme giuridiche, ma anche a valori di tipo etico può rappresentare un'opportunità. L'adozione di un *Modello Organizzativo* che renda le procedure interne più trasparenti, oltre a garantire l'esenzione dalla responsabilità amministrativa, costituisce infatti un'occasione di crescita e sviluppo per le imprese, migliorando, da un lato, il loro rapporto con la società e, quindi, la loro immagine pubblica e, dall'altro, riducendo i costi di transazione derivanti da eventuali azioni legali e da processi di contrattazione.

Pertanto, la Maticmind, sensibile all'esigenza di diffondere e consolidare la cultura della trasparenza e dell'integrità, nonché consapevole dell'importanza di assicurare condizioni di correttezza nella conduzione degli affari e nelle attività aziendali a tutela della propria posizione e immagine, adotta il presente Modello di Organizzazione e Gestione previsto dal Decreto, fissandone i principi di riferimento.

Il *Modello Organizzativo* Maticmind si pone, quindi, come obiettivo principale quello di configurare un sistema strutturato e organico di prescrizioni anche organizzative, procedure e attività di controllo, volto a prevenire, per quanto possibile, la commissione di condotte idonee a integrare i reati contemplati dal Decreto e a favorire una condotta appropriata da parte di tutte le parti. In altri termini, il presente *Modello Organizzativo* mira a:

- prevenire e ragionevolmente limitare i possibili rischi connessi all'attività aziendale con particolare riguardo alla scoperta e riduzione di eventuali condotte illegali
- determinare, in tutti coloro che operano in nome e per conto di Maticmind, nelle Aree di attività a Rischio, la consapevolezza di poter incorrere, nel caso di violazioni alle disposizioni riportate nel *Modello Organizzativo*, in un reato passibile di sanzioni penali e amministrative non solo nei loro confronti, ma anche nei confronti di Maticmind
- ribadire che Maticmind non tollera comportamenti illeciti, di ogni tipo e indipendentemente da qualsiasi finalità, in quanto gli stessi, oltre a trasgredire le leggi vigenti, sono comunque contrari ai principi etico-sociali cui Maticmind intende attenersi.

A tal fine il *Modello Organizzativo* si basa sui seguenti principi cardine:

- l'individuazione delle Attività a Rischio, ossia quelle attività nel cui ambito è stata riscontrata come più probabile la commissione dei reati previsti dal Decreto;
- la definizione e il costante aggiornamento di un Sistema Normativo Interno diretto a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai rischi-reato da prevenire e composto:
  - da una struttura organizzativa coerente tesa ad ispirare e controllare la correttezza dei comportamenti nel rispetto del principio di separazione delle funzioni, in base al quale nessuno può gestire in autonomia un intero processo
  - da un sistema di deleghe e di poteri aziendali sempre aggiornato che assicura una chiara e trasparente rappresentazione del processo aziendale di formazione e di attuazione delle decisioni

- da un *Codice Etico*, che fissa i principi ispiratori dell'azienda
- da un Codice Disciplinare, che riassume il complessivo regime sanzionatorio
- da procedure formalizzate, tese a disciplinare in dettaglio le modalità per assumere ed attuare decisioni nei settori "sensibili", con precisazioni riguardo la documentazione di ogni operazione rilevante
- da un'attività di formazione organica e strutturata finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. 231/2001, differenziata nei contenuti e nelle modalità di attuazione in funzione della qualifica dei destinatari e del livello di rischio dell'area in cui questi operano
- dall'attribuzione all'Organismo di Vigilanza di specifici compiti di vigilanza sull'efficace e corretto funzionamento del *Modello Organizzativo*, sulla coerenza di quest'ultimo rispetto agli obiettivi e sul suo aggiornamento periodico.

9.3 LE COMPONENTI DEL MODELLO ORGANIZZATIVO

Il *Modello Organizzativo* è rappresentato, oltre che dal presente documento, da altri specifici rappresentativi di alcuni ambiti, che completano e dettagliano il quadro della organizzazione, della gestione e del controllo della Società, tra i quali il *Codice Etico*, il *Codice Disciplinare*, l'*Analisi del Rischio*, il *Regolamento dell'Organismo di Vigilanza*.

Tali documenti unitariamente considerati costituiscono il *Modello Organizzativo* della Società, adottato ai sensi del Decreto 231/2001.

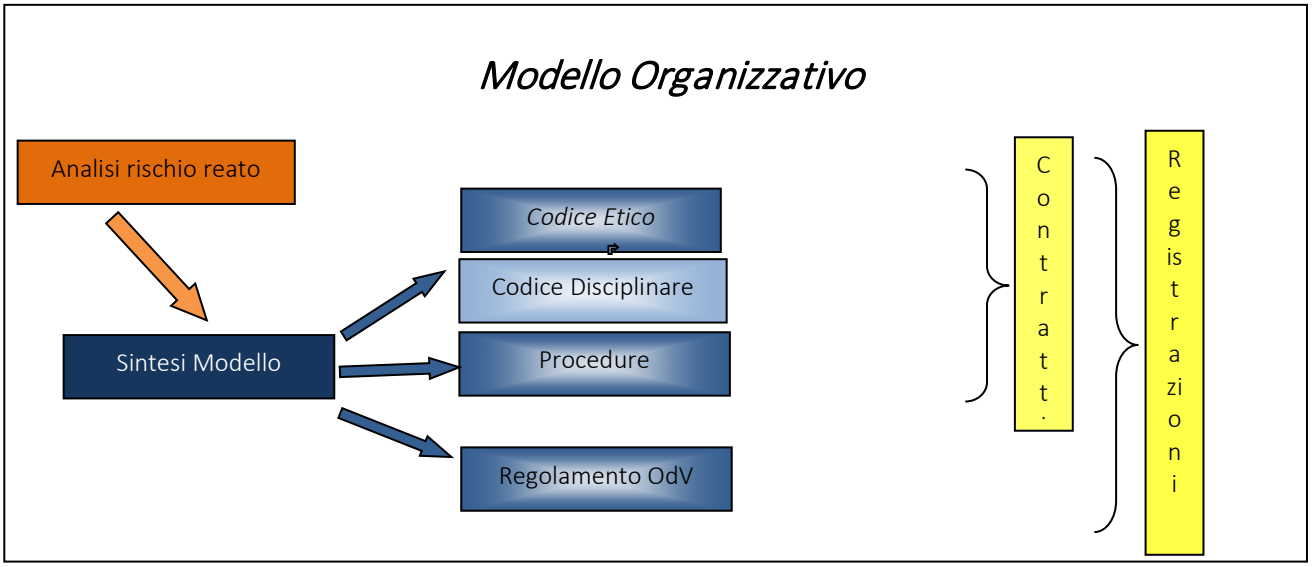


Figura 1: Struttura documentale del *Modello Organizzativo*

9.4 DESTINATARI DEL MODELLO ORGANIZZATIVO

Le regole contenute nel presente *Modello Organizzativo* si applicano a coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione e controllo in Maticmind (ossia, all'Organo Amministrativo, ai Dirigenti e ai Responsabili di funzione), ai Dipendenti, nonché a coloro i quali, pur non appartenendo all'Azienda operano su mandato della medesima o sono legati alla società da rapporti di Partnership, Fornitura e Consulenza.

Ove non diversamente e puntualmente specificato nel presente documento, negli altri documenti facenti parte del *Modello Organizzativo* e nel *Codice Etico*, si fa riferimento ai c.d. Destinatari del *Modello Organizzativo* per indicare tutti i soggetti sopra indicati.

9.5 DIFFUSIONE DEL MODELLO ORGANIZZATIVO

Maticmind comunica il presente *Modello Organizzativo* attraverso modalità idonee ad assicurarne l'effettiva conoscenza da parte di tutti i Destinatari dello stesso e in genere di tutti i soggetti che possono esserne interessati.

Al fine di agevolarne la conoscenza il presente *Modello Organizzativo* è pubblicato anche sul *Portale del Sistema di Gestione Integrato* (opzione "*Modello 231*").

9.6 L'AGGIORNAMENTO DEL MODELLO ORGANIZZATIVO

L'Organismo di Vigilanza ha il compito di promuovere il necessario e continuo aggiornamento ed adeguamento del *Modello Organizzativo* e dei protocolli ad esso connessi (ivi incluso il *Codice Etico*), suggerendo all'Organo Amministrativo, o alle funzioni aziendali di volta in volta competenti, le correzioni e gli adeguamenti necessari o opportuni.

Il Consiglio di Amministrazione è responsabile, unitamente alle funzioni aziendali eventualmente interessate, dell'aggiornamento del *Modello Organizzativo* e del suo adeguamento in conseguenza di mutamenti degli assetti organizzativi o dei processi operativi, di significative violazioni del *Modello Organizzativo* stesso e di integrazioni legislative.

Gli aggiornamenti e gli adeguamenti del *Modello Organizzativo* e dei protocolli ad esso connessi sono comunicati mediante apposite comunicazioni, inviate a mezzo @email e pubblicate sulla intranet aziendale e, se del caso, attraverso la predisposizione di sessioni formative/informative illustrative degli aggiornamenti e degli adeguamenti più rilevanti.

10 IL MODELLO DI GOVERNANCE

Alla luce della peculiarità della propria struttura organizzativa e delle attività svolte, Maticmind ha adottato il modello di amministrazione e controllo classico, ovvero basato sulla presenza di un Organo di Amministrazione formato da uno o più membri e un Collegio Sindacale. Il sistema di corporate governance della Maticmind risulta, pertanto, così articolato:

- Organo di Amministrazione, rappresentato dal Consiglio di Amministrazione costituito, in ottemperanza a quanto definito dall'art. 15 dello Statuto, da un minimo di 5 ad un massimo di 9 membri (cfr. Statuto – Titolo IV" Amministrazione della società" Art. 15)
- Consiglio di Amministrazione, a cui spetta in via esclusiva la gestione dell'impresa e la gestione di tutte le operazioni necessarie per l'attuazione dell'oggetto sociale
- Collegio Sindacale, composto, in ottemperanza a quanto definito dall'art. 23 dello Statuto, da 3 membri effettivi e da 2 sindaci supplenti (cfr. Statuto – Titolo VI "*Collegio Sindacale*" Art. 23)
- Revisore Contabile, incarico assunto da una Società di Revisione che esercita il controllo contabile (cfr. Statuto – Titolo VI "*Revisore*" Art. 24): in ottemperanza a quanto definito dall'art. 24 dello Statuto, è stato nominato un revisore esterno.

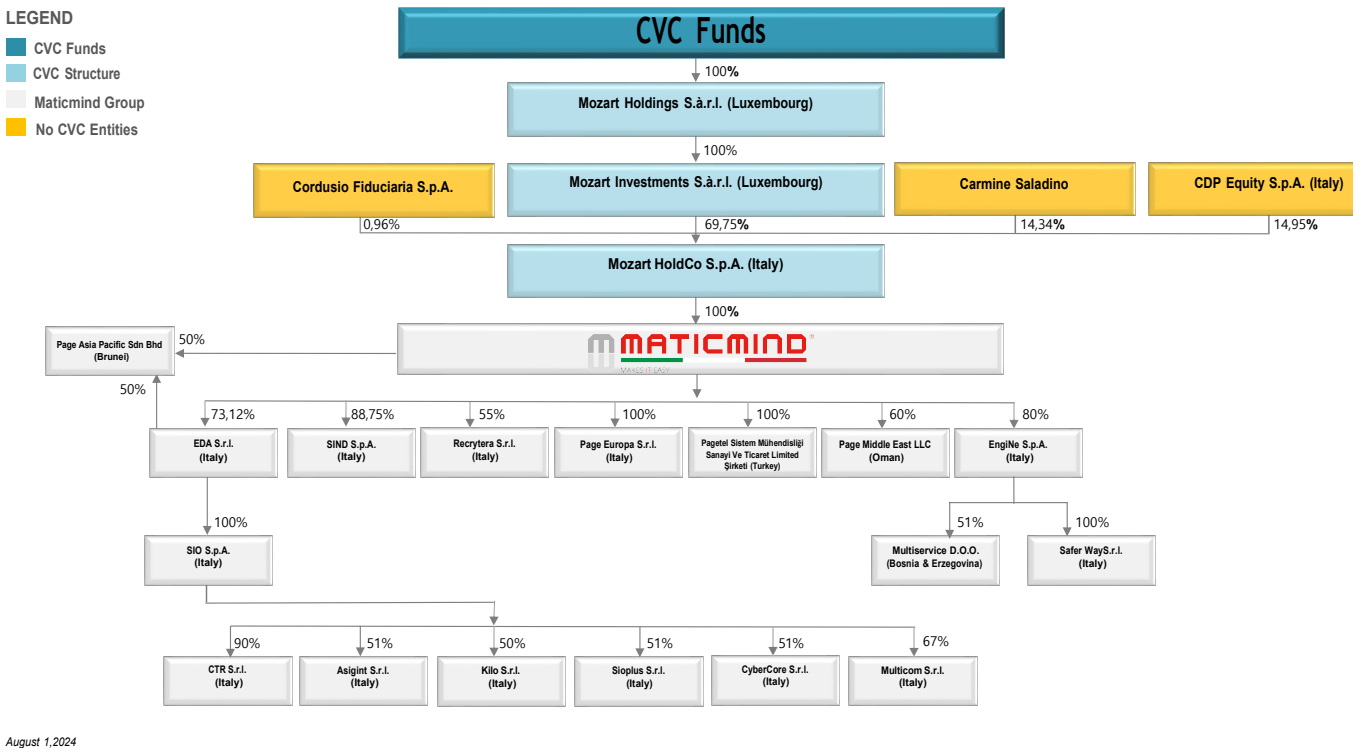
Maticmind promuove l'adozione ed efficace attuazione da parte di tutte le società controllate e partecipate di idonei sistemi di prevenzione del rischio di responsabilità amministrativa degli enti derivante da reato, in particolare sensibilizza ciascuna società controllata o partecipata (d'ora in avanti "Società del Gruppo) in merito all'importanza di dotarsi di un sistema di controllo interno aggiornato e idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri esponenti, dipendenti o apicali, partner e fornitori e di tutti coloro che operano nel suo interesse. Secondo quanto disciplinato negli strumenti normativi interni di Maticmind, le Società del Gruppo adottano e attuano, nella gestione delle attività a rischio ai fini della responsabilità amministrativa degli enti, principi e presidi di controllo coerenti con quanto previsto nel Modello 231 di Maticmind opportunamente adeguati tenendo conto della normativa applicabile, della specifica operatività dell'ente e della sua organizzazione. Nell'esercizio della propria autonomia, le singole Società del Gruppo sono responsabili dell'adozione e attuazione dei rispettivi Modelli 231 e/o altri modelli di compliance.

A questo proposito, si riporta di seguito il societogramma aggiornato di Gruppo, dal quale si evincono sia la catena di controllo della Società che le singole controllate e partecipate con le rispettive quote.

Segnatamente, dallo stesso si evince che la catena di controllo è così composta: il 100% delle azioni di Maticmind è posseduta dalla Mozart HoldCo S.p.A. persona giuridica di diritto italiano che, a sua volta, è controllata dal socio di maggioranza Mozart Investments S.à.r.l. con sede in Lussemburgo che ha il 69,75% del capitale, nonché dai soci di minoranza CDP Equity S.p.A. al 14,95%, Carmine Saladino al 14,34% e Cordusio Fiduciaria allo 0,96%.

La Mozart Investments S.à.r.l., a sua volta, è controllata al 100% dalla Mozart Holdings S.à.r.l. anch'essa di diritto lussemburghese, il cui capitale è interamente nelle mani di CVC Funds.

Tra le altre controllate, invece, con partecipazioni totalitarie o comunque maggioritarie spiccano le seguenti: SIO S.p.A., Sind S.p.A., Recrytera S.r.l., Page Europa S.r.l. ed EngiNe S.r.l..



10.1 L'ORGANIGRAMMA AZIENDALE: RUOLI E FUNZIONI

Maticmind ha definito la propria struttura organizzativa, vedere anche paragrafo 9.1.3, descritta attraverso:

- l'Organigramma aziendale (cfr. *MM_SGI_aaaammgg_Organigramma_Direzione Generale*), indicativo delle strutture direttive di primo livello e quelle di immediato riporto a queste ultime (funzioni)
- le principali funzioni aziendali (cfr. *MM_SGI_Descrizioni Funzioni Maticmind*)
- il mansionario delle figure professionali coinvolte nelle strutture definite (cfr. *MM_SGI_Schede Mansionario Aziendale*)

al fine di rendere immediatamente chiaro il ruolo e le responsabilità di ciascuno nell'ambito del processo decisionale aziendale.

Attraverso l'Organigramma è possibile individuare:

- le funzioni aziendali coinvolte nei principali processi di business e/o produttivi
- le linee di dipendenza gerarchica delle singole funzioni aziendali
- i soggetti che operano nelle singole aree ed il relativo ruolo organizzativo.

I documenti che specificano la struttura organizzativa, i ruoli e le funzioni aziendali sono stati predisposti dalla Direzione aziendale, responsabile del costante e puntuale loro aggiornamento in funzione dei cambiamenti effettivamente intervenuti nella struttura organizzativa.

L'organigramma, la descrizione delle funzioni ed il mansionario aziendale sono consultabili attraverso la rete intranet aziendale, accedendo al *Portale del Sistema di Gestione Integrato* (opzione Qualità e Service Management/Organizzazione Maticmind).

10.2 STRUTTURA ORGANIZZATIVA IN MATERIA DI SSL

Nell'ottica di eliminare ovvero ridurre e quindi gestire i rischi lavorativi per i propri dipendenti, in materia di Salute e Sicurezza sul Lavoro, la Società si è dotata di una struttura organizzativa (vedi Organigramma SSL *MM_8108_aaaammgg_Organizzazione Sicurezza*) conforme a quella prevista dalla normativa prevenzionistica vigente (D.Lgs. 81/2008). Ha inoltre definito una funzione specifica di *Safety & Facility Management* che ha la responsabilità di:

- supportare il RSPP e le altre strutture aziendali impegnate nell'erogazione delle attività operative presso le sedi dei Clienti, affinché queste ultime siano effettuate nel rispetto degli standard definiti di sicurezza interna (vedi procedura di *Gestione Sicurezza negli Appalti*)
- assicurare il rispetto delle regole di prevenzione e sicurezza nelle sedi Maticmind, in aderenza agli standard internazionali ISO e alla norma prevenzionistica vigente (D.Lgs. 81/2008).

10.3 STRUTTURA ORGANIZZATIVA PER LA SICUREZZA DELLE INFORMAZIONI

L'organizzazione per la gestione della *Sicurezza delle Informazioni* è funzionale all'individuazione delle politiche dirette alla gestione e al controllo delle misure adottate e si concretizza nella definizione di ruoli, funzioni e responsabilità coinvolte nella realizzazione e gestione del sistema omonimo.

La governance della Sicurezza delle Informazioni è responsabilità della Direzione Generale, che si avvale del supporto del *Comitato Direttivo per la Sicurezza (CDS)* per la definizione e attuazione delle politiche e delle linee guida di sicurezza delle informazioni, per la designazione dei ruoli e delle responsabilità di primo livello del Sistema di Gestione della Sicurezza delle Informazioni, nonché per l'identificazione delle risorse e degli investimenti da sostenere in ottica miglioramento. Il CDS vede la partecipazione dei seguenti membri stabili:

- Amministratore Delegato
- Direttore Operation
- Responsabile della Sicurezza delle Informazioni (CISO)
- Responsabile della Protezione dei Dati Personali (DPO).

Il CDS si riunisce con cadenza semestrale, ma su richiesta dell'Amministratore Delegato può attuare incontri "ad evento" e/o con una frequenza superiore a quella semestrale. La partecipazione al CDS può essere estesa, in base alle esigenze e alle problematiche da esaminare, a ruoli operativi e, in generale, ai diversi responsabili delle funzioni aziendali.

A livello operativo, al fine di assicurare la corretta attuazione delle politiche e delle linee guida per la sicurezza delle informazioni e garantire l'efficienza e l'efficacia del Sistema di Gestione della Sicurezza delle Informazioni, la Direzione Generale ha definito una struttura organizzativa che comprende le figure di:

- Responsabile Sicurezza delle Informazioni (CISO)
- Responsabile della Protezione dei Dati Personali (DPO)
- Internal Auditor
- Facility Security Manager
- Responsabile del Centro Operativo per la Sicurezza (SOC)
- Responsabili delle Funzioni Aziendali

10.4 IL SISTEMA DI PROCURE E DELEGHE

10.4.1 I PRINCIPI GENERALI

Il Consiglio di Amministrazione di Maticmind è l'organo preposto a conferire e approvare formalmente le deleghe e i poteri di firma, con puntuale indicazione delle soglie di approvazione delle spese assegnate, in coerenza con le responsabilità organizzative e gestionali definite, così come richiesto dalla buona pratica aziendale e specificato anche nell'ultima versione del giugno 2021 delle Linee Guida di Confindustria.

Il livello di autonomia, del potere di rappresentanza e i limiti di spesa assegnati ai vari titolari di deleghe e procure all'interno della Società sono sempre individuabili e fissati:

- in modo coerente con il livello gerarchico del destinatario della delega o della procura
- nei limiti di quanto strettamente necessario all'espletamento dei compiti e delle mansioni oggetto di delega
- in base alla dimensione del business gestito.

I poteri così conferiti sono periodicamente aggiornati in funzione dei cambiamenti organizzativi o strategici che intervengono nella struttura della Società, che ha inoltre istituito un flusso informativo nei confronti di tutte le funzioni e soggetti aziendali, al fine di garantire la tempestiva comunicazione dei poteri e dei relativi cambiamenti (a qualsiasi titolo interessati, incluso l'Organismo di Vigilanza e il Collegio Sindacale).

10.4.2 LA STRUTTURA DEL SISTEMA DI DELEGHE E PROCURE IN MATICMIND

Con il Verbale del Consiglio di Amministrazione del 28/4/2017 sono stati definiti i poteri conferiti all'Amministratore Delegato e i relativi poteri di firma ad esso riconosciuti per specifiche operazioni di gestione.

In atti successivi sono state ratificate le procure e i relativi poteri di firma precedentemente rilasciate a definiti procuratori, nonché gli atti da essi svolti fino a quella data in virtù delle stesse.

Le procure rilasciate al Consiglio di Amministrazione e al Direttivo, in termini di soggetti delegati e di poteri di firma ad essi riconosciuti sono formalizzati ed ufficializzati, per le procure depositate, nella Visura Camerale della società e nei relativi documenti interni per le altre, cui si rimanda per un adeguato dettaglio.

Qualora la Società e il suo rappresentante legale siano contestualmente indagati per il medesimo reato presupposto di cui al D.Lgs. n. 231 del 2001, la nomina del difensore per l'assistenza e la rappresentanza in giudizio di Maticmind dovrà essere conferita mediante delibera del Consiglio di Amministrazione ed eventuale procura speciale ad un suo componente per le conseguenti sottoscrizioni.

10.5 IL SISTEMA DI GESTIONE AZIENDALE

Nell'ambito del proprio sistema organizzativo, Maticmind ha messo a punto un *Sistema di Gestione* (*Sistema di Gestione Integrato*) che comprende politiche, linee guida, standard, *template* e procedure volto a regolamentare lo svolgimento delle attività aziendali, nel rispetto dei principi indicati dalle disposizioni interne, dalla normativa vigente (D.lgs. 231/2001 e D.Lgs. 81/2008) e dagli standard internazionali di

riferimento (ISO9001:2015, ISO20000:2018, ISO27001:2013, ISO27017, ISO27018, ISO45000:2018; ISO14001, ISO14064-1, ISO37001, PDR125).

Le procedure approntate descrivono le regole da seguire in seno ai processi aziendali interessati, garantendo la correttezza, l'efficacia e l'efficienza delle attività aziendali attraverso l'indicazione:

- delle attività del processo
- degli input e output
- delle responsabilità
- dei flussi informativi
- dei documenti e/o i sistemi informativi a supporto
- dei controlli inerenti all'efficacia e all'efficienza.

I principali processi aziendali di business e gestionali riferiti alle aree commerciali, agli acquisti, alla logistica e alla delivery sono supportati dal *Sistema Informativo aziendale SIM*, che costituisce la "guida" del flusso di lavoro (workflow), assicurando così un elevato livello di standardizzazione e di compliance. Il sistema informativo aziendale fornisce supporto soprattutto:

- durante il processo di Pre-Vendita, relativamente alla gestione dei flussi di approvazione delle Offerte formalizzate
- nel processo di Vendita, per la gestione degli Ordini dei Clienti e l'assegnazione delle attività operative
- per l'emissione degli Ordini a fornitori, in termini di gestione dei flussi di approvazione delle Richieste di Acquisto
- alla gestione della logistica e del magazzino (carico e scarico delle merci e movimentazione interna)
- alla gestione della delivery, assicurando la tracciabilità dell'intero ciclo produttivo
- alla gestione finanziaria, di Controllo e Reporting.

Per maggiore chiarezza l'Allegato 2, parte integrante del presente documento, riporta la tabella di correlazione tra la documentazione del Sistema di Gestione Integrato, i punti del D.Lgs. 231 e quelli relativi agli standard ISO di riferimento.

10.6 IL SISTEMA DI CONTROLLO

Il sistema di controllo di Maticmind, finalizzato alla prevenzione del rischio di commissione dei reati previsti dal D.Lgs. 231/2001, affianca l'osservanza del *Codice Etico*, principio generale non derogabile del Modello 231, e si basa sulle attività di verifica e di monitoraggio tipiche del Sistema di Gestione Aziendale, nel quale sono recepiti i principi di cui agli standard internazionali UNI EN ISO e al D.Lgs. 81/2008.

Il sistema di controllo prevede meccanismi di verifica dell'osservanza:

- dell'andamento delle attività lavorative (monitoraggio)
- delle policy e delle procedure aziendali nel corso delle attività lavorative, volta a garantire l'efficacia, l'efficienza e la tracciabilità delle azioni intraprese e dei risultati conseguiti
- delle normative vigenti
- delle responsabilità di chi esegue, controlla e autorizza le attività e/o i prodotti da esse derivati

- delle disposizioni aziendali idonee a fornire i principi di riferimento generali per la regolamentazione dell'attività
- dei poteri di delega riconosciuti alle funzioni competenti.

Tali controlli sono eseguiti attraverso la regolare attività di **sorveglianza**, svolta dal Responsabile del *Sistema di Gestione Integrato* (funzione *Assicurazione Qualità* e *Internal Auditor Sicurezza*) e dal personale qualificato facente parte dell'*Organismo di Vigilanza* (o da questi incaricato) attraverso:

- **audit interni**
- **Riesami** periodici limitatamente al D. Lgs. 231/2001 (della Direzione o dell'Organismo di Vigilanza)
- verifica periodica dell'esito dei controlli effettuati in sede di **revisione contabile**.

L'attività di sorveglianza e di controllo è condotta dai soggetti incaricati in forma pianificata o estemporanea.

10.7 IL SISTEMA DI CONTROLLO DELLA SALUTE E SICUREZZA SUL LAVORO

10.7.1 LA GESTIONE OPERATIVA IN MATERIA SSL

La gestione degli aspetti relativi alla *Salute ed alla Sicurezza sul Lavoro* è effettuata con l'obiettivo di provvedere in via sistematica:

- all'identificazione dei rischi e alla loro valutazione, affinché siano eliminati ovvero, ove ciò non sia possibile, siano ridotti al minimo e quindi gestiti
- alla riduzione minima del numero di lavoratori esposti a rischi
- all'individuazione delle misure di prevenzione e di protezione adeguate rispetto ai rischi riscontrati
- alla definizione di adeguate misure di protezione collettiva e individuale, fermo restando che le prime devono avere priorità sulle seconde
- al controllo sanitario dei lavoratori in funzione dei rischi specifici
- alla programmazione della prevenzione, considerando in modo coerente e integrato le condizioni tecniche e produttive dell'azienda, con l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro
- alla realizzazione di interventi programmati finalizzati alla prevenzione e protezione collettiva e individuale
- alla formazione e addestramento delle figure professionali previste dalle norme relative alla SSL (81/2008), nei limiti dei rispettivi ruoli, funzioni e responsabilità
- alla comunicazione del *Modello Organizzativo* ai destinatari, nei limiti dei rispettivi ruoli, funzioni e responsabilità, in modo da assicurare il livello di coinvolgimento adeguato
- alla regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo ai dispositivi di sicurezza, in conformità alle indicazioni dei fabbricanti.

10.7.2 IL SISTEMA DI MONITORAGGIO DELLA SICUREZZA

La Società ha rivolto particolare attenzione all'esigenza di predisporre e implementare, in materia di *Salute e Sicurezza sul Lavoro*, un efficace ed efficiente sistema di controllo conforme alle disposizioni vigenti in materia.

Il primo livello di monitoraggio coinvolge tutti i soggetti che operano nell'ambito della struttura organizzativa della Società, che sono tenuti in prima persona al rispetto delle disposizioni in materia di Salute e Sicurezza sul Lavoro e alla segnalazione al diretto Responsabile di eventuali anomalie riscontrate durante lo svolgimento delle attività di propria competenza.

Il secondo livello di monitoraggio è svolto dalla funzione *Assicurazione Qualità* e dall'*Organismo di Vigilanza*, ai quali è assegnato il compito di verificare la funzionalità, l'efficacia ed efficienza del Sistema di Salute e Sicurezza sul Lavoro adottato dalla Maticmind a tutela dei lavoratori. Tale compito è stato assegnato alla funzione *Assicurazione Qualità* e all'*Organismo di Vigilanza* in ragione della loro idoneità ad assicurare efficacia, obiettività e imparzialità dell'operato, nonché l'indipendenza dal settore di lavoro sottoposto a verifica ispettiva.

L'attività di controllo è eseguita attraverso l'analisi dell'andamento dei risultati conseguiti, anche ad altri fini e/o mediante la conduzione di audit interni. Nell'effettuazione degli audit l'*Organismo di Vigilanza* può usufruire della competenza di personale esterno all'organismo appositamente incaricato.

10.8 SISTEMA DI CONTROLLO PER LA SICUREZZA DELLE INFORMAZIONI

10.8.1 LA GESTIONE OPERATIVA IN MATERIA SICUREZZA

Il *Responsabile della Sicurezza delle Informazioni*, con la collaborazione dei singoli Responsabili delle Funzioni aziendali (vedi Organigramma *MM_aaaammgg_Organigramma Direzione Generale*). garantisce l'attuazione delle politiche, delle procedure, delle regole e dei criteri relativi al *Sistema di Sicurezza delle Informazioni* attraverso:

- il coordinamento e la gestione delle risorse umane e tecnologiche, della sicurezza logica e fisica di Maticmind;
- la gestione dei rapporti con i fornitori esterni di servizi informatici di ambito;
- l'individuazione e attuazione degli adeguati requisiti di sicurezza informatica nelle fasi di progettazione, implementazione e rilascio di nuove applicazioni/infrastrutture informatiche, nonché nelle fasi di manutenzione (correttiva e/o evolutiva) di quelle esistenti;
- l'assicurazione del pieno rispetto delle disposizioni, anche legislative, vigenti in materia di sicurezza dell'informazione e protezione dei dati personali;
- la diffusione della conoscenza delle politiche di sicurezza e la formazione del personale aziendale sul proprio ruolo e sulle proprie responsabilità nell'ambito della sicurezza delle informazioni;
- l'autorizzazione dei dipendenti all'uso delle risorse informative necessarie alle attività di cui sono responsabili e l'opportuna formazione sull'utilizzo di queste ultime;
- l'organizzazione della "struttura di sicurezza aziendale" finalizzata a prevenire e proteggere, in armonia con le misure stabilite, il complesso degli archivi, delle procedure e dei sistemi, da minacce ed eventi critici.

L'Internal Auditor della Sicurezza è responsabile del monitoraggio complessivo del Sistema di Gestione della Sicurezza delle Informazioni, al fine di assicurare l'efficienza del sistema e l'efficacia degli strumenti di cui è composto. Attraverso la regolare attività di **sorveglianza**, svolta mediante **audit interni**, rileva possibili non

conformità, rischi e azioni di miglioramento finalizzate alla correzione e/o perfezionamento del sistema. Analogamente al *Responsabile della Qualità*, partecipa ai Riesami periodici della Direzione.

Il *Responsabile del Facility Management*, in collaborazione con il Responsabile della Sicurezza delle Informazioni, ha la responsabilità della gestione operativa dei servizi inerenti la Sicurezza Fisica e Ambientale, tra cui:

- la gestione degli accessi fisici alle sedi aziendali e alle aree ad accesso ristretto e controllato
- lo sviluppo, l'implementazione e la gestione operativa dei servizi inerenti alla rilevazione di incendi e/o allagamenti, i sistemi di continuità elettrica (UPS), i sistemi di controllo del livello di temperatura ambientale e di umidità
- la gestione dei piani di emergenza nei luoghi di lavoro.

Il *Responsabile della Protezione dei Dati Personali (DPO)* ha la responsabilità di informare e supportare il Titolare del Trattamento in merito agli obblighi derivanti dal regolamento e supervisionare che la conformità al regolamento sia osservata. In particolare, è tenuto a:

- sviluppare e attuare una politica di protezione dei Dati Personali adeguata e assicurarsi che quest'ultima sia rivista con cadenza periodica
- sviluppare e attuare processi e procedure relative alla protezione dei dati personali
- fungere da *focal point* per gli interessati nel caso in cui essi vogliano far valere i propri diritti e all'occorrenza gestire i reclami e i ricorsi
- eseguire regolarmente audit interni e supportare quelli esterni per verificare la conformità con il regolamento e le relative politiche organizzative
- assicurarsi che l'organizzazione disponga di sistemi di controllo, tecnici e organizzativi, adeguati ai rischi incombenti sul trattamento
- fornire consulenza e formazione al personale e ai dirigenti dell'Azienda affinché siano educati in materia di protezione dei dati personali

Il *Responsabile Centro Operativo per la Sicurezza (SOC)* rappresenta la figura apicale dell'organo deputato ad affrontare e risolvere le problematiche di carattere operativo che possono insorgere, sia nelle attività di definizione e miglioramento del *Sistema di Gestione per la Sicurezza delle Informazioni*, che nell'attuazione dello stesso. Ha inoltre la responsabilità di monitorare e analizzare gli eventi di sicurezza, gestendo i potenziali e/o effettivi incidenti di sicurezza e di gestire le configurazioni degli apparati di sicurezza aziendali, utilizzati per il rilevamento degli incidenti di sicurezza.

10.9 COMUNICAZIONE FORMAZIONE E ADDESTRAMENTO DEL PERSONALE

10.9.1 COMUNICAZIONE E COINVOLGIMENTO

La Società promuove la più ampia divulgazione dei principi e delle previsioni contenuti nel *Modello Organizzativo* e negli altri documenti parte integrante dello stesso, coinvolgendo tutto il personale aziendale attraverso gli strumenti di comunicazione predisposti. La promozione e comunicazione del *Modello*

Organizzativo nei limiti dei rispettivi ruoli, funzioni e responsabilità dei destinatari coinvolti comprende anche gli aspetti connessi alla Salute e Sicurezza sul Lavoro.

Per i Terzi Destinatari tenuti al rispetto del *Modello Organizzativo* è resa disponibile sul sito internet della Società una sintesi dello stesso per ciò che concerne gli aspetti per essi rilevanti.

Al fine di formalizzare ulteriormente l'impegno da parte di Terzi Destinatari al rispetto dei principi del *Modello Organizzativo* e dei documenti ad esso connessi, la Società prevede l'inserimento di una apposita clausola nel contratto di riferimento con essi stipulato e la sottoscrizione di una specifica pattuizione integrativa al contratto stesso.

L' Organismo di Vigilanza monitora tutte le ulteriori attività di informazione che dovesse ritenere necessarie o opportune.

10.9.2 FORMAZIONE E ADDESTRAMENTO

In aggiunta alle attività connesse di comunicazione e informazione verso i Destinatari, l'Organismo di Vigilanza ha il compito di curare la periodica e costante formazione di questi ultimi, ovvero promuovere e monitorare l'implementazione per conto della Società di iniziative volte a favorire una conoscenza e una consapevolezza adeguate del Modello Organizzativo e dei documenti ad esso connessi, al fine di incrementare la cultura di eticità all'interno della Società stessa.

Attraverso la predisposizione di appositi piani formativi approvati dal Consiglio di Amministrazione, Maticmind eroga la formazione e l'addestramento dei Destinatari del *Modello Organizzativo* nelle questioni connesse alla sua gestione, nei limiti dei rispettivi ruoli, funzioni e responsabilità. Tale attività è finalizzata ad assicurare un'adeguata consapevolezza sull'importanza della conformità delle azioni rispetto al *Modello Organizzativo* e delle possibili conseguenze connesse a violazioni dello stesso.

In quest'ottica è data particolare rilevanza alla formazione e all'addestramento dei soggetti che svolgono compiti in materia di gestione, per garantire una corretta divulgazione e conoscenza delle regole di condotta contenute nei confronti sia delle risorse già presenti, sia di quelle da inserire in organico, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento dei soggetti nelle attività a rischio.

Le modalità di svolgimento delle attività di formazione e informazione, necessarie a garantire anche la corretta applicazione delle disposizioni previste nel Decreto, sono diversificate a seconda dei soggetti interessati e attuate in momenti differenti della vita aziendale dei Destinatari. L'adozione del presente *Modello Organizzativo* è comunicata comunque a tutte le risorse operanti in Azienda, che devono sottoscrivere un apposito modulo per presa conoscenza e accettazione del Modello Organizzativo e del Codice Etico ad esso correlato: entrambe i documenti sono reperibili attraverso la sezione intranet dedicata sul *Portale del Sistema di Gestione Integrato*.

Ai **nuovi assunti** l'adozione è comunicata mediante un set documentale costituito dal CCNL, dal presente documento *Modello di Organizzazione e Gestione* e dal *Codice Etico*, consegnato tramite dotazione cartacea o informatica, con il quale si assicura agli stessi le conoscenze considerate di primaria rilevanza.

Ai **dipendenti** già presenti in azienda il *Modello Organizzativo* e il *Codice Etico* ad esso correlato sono comunicati formalmente al momento dell'adozione del Modello.

All'**Organo Amministrativo** è consegnata copia del presente documento *Modello di Organizzazione e Gestione* e del *Codice Etico*, che devono essere sottoscritti in aggiunta al modulo per presa conoscenza e accettazione e a una dichiarazione di assenza di conflitti di interesse.

Per i **Consulenti** è prevista la consegna da parte delle funzioni aventi contatti con tali soggetti di una copia del *Modello Organizzativo* e del *Codice Etico*, nonché di una idonea informativa sulle conseguenze del mancato rispetto del *Modello Organizzativo* stesso.

Nel periodo successivo all'adozione del *Modello Organizzativo* è pianificata, condivisa con gli interessati ed erogata una specifica attività di formazione "continua", attraverso sia strumenti e procedure informatiche (Intranet aziendale, e-mail di aggiornamento) che incontri e seminari di formazione e aggiornamento.

Tale attività formativa e informativa è differenziata nei contenuti e nelle modalità di erogazione in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano e dell'assunzione o meno di funzioni di rappresentanza della Società.

La partecipazione alle attività di formazione è obbligatoria.

Delle attività di formazione è redatto un verbale riepilogativo archiviato presso la struttura documentale del *Sistema di Gestione Integrato*.

10.10 SEGNALAZIONI DI REATI O IRREGOLARITA'

Il 29 dicembre 2017 è entrata in vigore la Legge n. 179 recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato", a cui si è aggiunta la recentissima normativa prevista dal D.Lgs. 10.3.2023 n. 24 (di recepimento della Direttiva UE 2019/1937), la quale ha riformato interamente la disciplina relativa alla protezione delle persone che segnalano violazioni del diritto dell'Unione e delle disposizioni normative nazionali.

Detta disciplina mira a incentivare le segnalazioni di illeciti da parte dei lavoratori, di cui gli stessi siano venuti a conoscenza nell'ambito del proprio contesto lavorativo, tramite l'istituzione di canali di segnalazione ad hoc, venendo comunque garantita la riservatezza dell'identità del soggetto segnalante nonché la sua tutela da eventuali ritorsioni.

Con l'espressione "whistleblower", dunque, si fa riferimento a una persona che segnala condotte illecite, di cui è venuto a conoscenza nell'ambito del proprio contesto lavorativo, mentre con "whistleblowing" si intende la disciplina volta a incentivare le segnalazioni e a tutelare il whistleblower, tenendolo indenne da eventuali comportamenti ritorsivi connessi alla segnalazione effettuata.

Maticmind ha dato attuazione al dettato normativo con il documento "MM_PAQ231_04_WHISTLEBLOWING POLICY", parte integrante del presente Modello, a cui si rimanda.

11 L'ANALISI DEL RISCHIO

L'analisi del rischio reato è stata articolata in aderenza alla linea guida internazionale per la "*Gestione dei Rischi*" (*ISO 31000:2018*) e al processo di *Risk Management* adottato dalla Società, che gestisce i rischi a cui deve far fronte attraverso le fasi sequenziali di seguito riportate. Il processo include inoltre il continuo *Monitoraggio e Riesame* dei rischi (*verifica dei controlli*) al fine di evitare che questi degenerino senza dare possibilità alla Società di organizzarsi e mettere in atto le dovute azioni di trattamento e/o copertura:

- *identificazione* delle aree di attività più esposte al rischio di commissione dei reati considerati dal Decreto (cfr. Analisi del rischio – Attività a rischio Sezione 5)
- *analisi*, *valutazione* e *trattamento* del livello di rischio di commissione dei reati nell'ambito delle aree considerate significative (cfr. Analisi del rischio – Livello di rischio Sezione 6 "Livello rischio Lordo")
- *verifica dei controlli* già esistenti (cfr. Analisi del rischio – Livello di rischio Sezione 6 "As-Is analysis").

11.1 IDENTIFICAZIONE DELLE AREE DI RISCHIO E REATI APPLICABILI

Nella redazione del *Modello Organizzativo* è stata effettuata:

- l'analisi della documentazione in essere
- l'analisi delle aree organizzative e gestionali più esposte all'interno delle quali, per la tipologia di attività svolta potrebbero essere commessi i reati presupposto rilevanti ai fini della responsabilità amministrativa di impresa
- un approfondimento con i referenti dei processi
- ove necessarie interviste condotte con i responsabili dei processi ritenuti critici ai fini del D.Lgs 231/2001

escludendo le aree aziendali per le quali la Società ha già posto in essere i controlli considerati ai fini dell'analisi in essere.

L'analisi delle aree di attività più esposte al rischio è stata condotta su tutte le attività che prevedono un contatto e/o un'interazione tra Maticmind ed i soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio, nonché sulle attività potenzialmente esposte al rischio di commissione dei reati Societari e, in generale, dei reati indicati dal Decreto (significativi).

Sulla base delle risultanze emerse da tale analisi è stato redatto il documento "Descrizione dei Reati" al fine di poter contare su un supporto adeguato a condividere con gli attori coinvolti l'ambito di intervento del Decreto e il livello di applicabilità dello stesso alle attività aziendali: in tale documento sono stati esplicitate le singole fattispecie di comportamento illecito per ogni categoria di reato presupposto ex D.Lgs. 231/2001 contemplate e la definizione dell'applicabilità alle attività della Maticmind.

Contestualmente è stata eseguita una "mappatura" delle aree aziendali in cui potrebbero essere commessi i reati rilevanti per il D.Lgs. 231/2001, con particolare attenzione all'individuazione delle funzioni che, per ruolo attribuito e poteri esercitati, potrebbero compiere le condotte vietate dalla citata normativa. Gli esiti di tale attività sono stati formalizzati nel § 12 "*MODELLI OPERATIVI*".

ai reati previsti dal Decreto sono state esclusi dal perimetro valutativo quelli che già nella fase preliminare di analisi sono risultati essere non significativi in quanto caratterizzati da livelli particolarmente limitati di:

- possibilità di commissione rispetto alla particolare attività analizzata
- potenziale interesse o vantaggio per il singolo e per la società.

Al fine di prevenire la commissione dei reati sanzionati dal D.Lgs. 231/2001 nel medesimo § 12 "*MODELLI OPERATIVI*" sono state valutate le diverse modalità con cui nelle diverse aree e competenze esaminate potrebbero essere concretamente commessi i reati previsti dal Decreto.

L'individuazione delle aree più esposte è monitorata costantemente al fine di identificare con la massima precisione possibile le modalità con cui potrebbero essere realizzate le condotte vietate dal D.Lgs. 231/2001.

È rivolta particolare attenzione agli impatti sulla struttura organizzativa, gestionale e di controllo determinati dalle eventuali variazioni organizzative, dagli aggiornamenti della normativa nonché da particolari situazioni (precedenti violazioni, eccessivo turnover del personale, ecc.): questi potrebbero portare all'identificazione di ulteriori rischi e conseguentemente alla modifica e/o integrazione del presente *Modello Organizzativo* e delle relative procedure ad esso connesse.

La necessità di aggiornamento e/o variazione del presente *Modello Organizzativo* e delle relative procedure ad esso connesse può nascere anche a valle delle ordinarie attività di monitoraggio e di controllo periodico condotte dall'Organismo di Vigilanza e in occasione degli audit interni effettuati.

Qualunque variazione organizzativa, aggiornamento della normativa e identificazione di ulteriori rischi è formalizzata attraverso l'aggiornamento dei *Modelli Operativi* (vedi § 12).

11.2 Valutazione del Livello di Rischio

Il livello di rischio delle attività è stato misurato facendo riferimento a due indicatori:

1. **Gravità** indicante la presumibile entità del danno che Maticmind potrebbe subire qualora se ne accerti la responsabilità
2. **Probabilità** da intendersi come la probabilità che nell'esercizio di una certa attività sia commesso un illecito penale rilevante ai sensi del Decreto.

Il fattore che ha influenzato la variabilità dell'indicatore di "**Gravità**" è stata la tipologia di reati astrattamente riconducibili alla attività oggetto di valutazione, unitamente alla considerazione delle sanzioni irrogabili. Altri fattori che hanno contribuito alla valorizzazione di questi due indicatori rispetto a ciascuna attività esaminata sono stati:

- la tipologia di relazione con la Pubblica Amministrazione
- il livello di discrezionalità
- la grandezza dei valori economici coinvolti
- il numero di soggetti abilitati ad esercitare l'attività e loro autonomia
- i fattori ambientali

Ad ogni attività è stato associato un livello di:

- **Gravità**, articolata su 3 livelli (alta/media/bassa)

- **Probabilità**, articolata su 3 livelli (alta/media/bassa).

Il prodotto di questi due fattori ha portato a definire il livello di rischio potenziale relativo ad ogni attività esaminata sulla base della tabella di seguito riportata.

		Gravità		
		1	2	3
Probabilità	1	1	2	3
	2	2	4	6
	3	3	6	9

Legenda: Gravità 1 = Bassa 2 = Media 3 = Alta

Probabilità 1 = Bassa 2 = Media 3= Alta

Rischio = Basso = Medio = Alto

La definizione di tale livello di rischio è stata formalizzata nei *Modelli Operativi* (vedi § 12).

11.3 Trattamento del Rischio

Le opzioni di trattamento dei rischi sono scelte sulla base del valore del rischio determinato durante la fase di *Risk Assessment* e sulla base dei costi e benefici stimati per l'implementazione delle opzioni di trattamento scelte (vedi *MM_SGI_Metodologia di Analisi dei Rischi*). Il valore associato a ciascun rischio è rappresentato dal risultato del prodotto tra **Probabilità** di commissione della fattispecie di reato contemplato dal D.Lgs. 231/2001 e la **Gravità** delle conseguenze dell'evento dannoso una volta che questo si sia verificato.

Il rischio è ritenuto "*Accettabile*" quando il valore del prodotto evidenzia un rischio basso, tale per quest'ultimo è accettato e non risulta di conseguenza opportuno intraprendere Azioni per minimizzare la probabilità e/o l'impatto potenziale del rischio, accettando le conseguenze del verificarsi del rischio stesso. La decisione dell'accettazione dei rischi è presa qualora i rischi risultino tollerabili, ovvero per tutti quei livelli di rischi determinati al di sotto della soglia di accettabilità stabilita nei *Criteri per Gestione del Rischio*. La scelta di accettazione del rischio è giustificata e documentata dall'OdV in corrispondenza di ciascun rischio individuato (vedi § 12 *Modelli Operativi*).

Questi non garantirebbero comunque un aumento significativo del livello di protezione dell'operatività aziendale in termini di esclusione della possibilità che si verifichi il rischio di mancata aderenza al Modello Organizzativo e al D.Lgs. 231/2001.

11.4 Verifica dei Controlli già Esistenti

Tutte le attività risultate a rischio alto e medio sono state sottoposte ad un'ulteriore verifica, mirata ad accertare che in tali aree i sistemi di controllo preventivo già in essere fossero conformi alle previsioni e finalità del Decreto. In particolare si è mirato ad accertare l'adeguatezza dei protocolli esistenti, ossia:

- la loro capacità di prevenire il verificarsi di comportamenti illeciti (o comunque, di ridurne il rischio ad un livello accettabile) e di evidenziarne l'eventuale realizzazione
- la rispondenza tra i comportamenti concreti e quelli formalmente previsti dai protocolli stessi.

La verifica condotta è stata formalizzata nel documento di Analisi del rischio – Livello di rischio Sezione 6 "As-Is analysis". In tale ambito tra i protocolli esistenti sono stati considerati quelli idonei a rappresentare previo eventuale adeguamento gli elementi costitutivi del Modello:

- sistema organizzativo
- policies, procedure e sistema di controlli
- sistema delle deleghe di poteri e delle procure
- comunicazione e formazione.

11.5 Definizione dei Controlli interni

E' stata effettuata una revisione dell'Analisi del rischio ("Rischio Netto") sulla base della rilevazione del grado di adeguatezza e effettività delle Procedure in essere e dei Controlli Interni, al fine di verificare la capacità di tali controlli di ridurre il rischio a livello basso ("Accettabile").

A conferma della definizione e implementazione dei controlli ritenuti idonei ad attestare il livello di rischio più "basso" per tutte le aree significative, è stato effettuato un ulteriore aggiornamento dell'Analisi del rischio (vedi "Rischio Netto").

11.6 Formazione Specifica per le Aree a Rischio

Per i dipendenti che operano nelle aree identificate a rischio "alto", è stata prevista una formazione specifica – svolta nel rispetto di quanto previsto al § 10.9.2 del presente documento - volta a sensibilizzare i soggetti coinvolti rispetto ai reati ascrivibili alla loro area di pertinenza, ai principi etici ad esso connessi e alle procedure definite dall'Azienda per la gestione dei relativi processi.

12 MODELLI OPERATIVI

Sono di seguito riportati i Modelli Operativi definiti sulla base delle risultanze dell'analisi del rischio-reato: è stato identificato, per ogni reato significativo, il rischio "assoluto" o "lordo", ossia quello derivante dal prodotto dei valori associati alla **Gravità** e alla **Probabilità** di commissione del reato, senza prendere in considerazione i controlli interni già in essere in azienda. Il rischio "relativo" o "netto" deriva, invece, dall'impatto sul livello di rischio "lordo" dei controlli già operativi e rappresenta quindi il livello di rischio contestualizzato nella realtà aziendale.

Indebita Percezione di Erogazioni, Truffa In Danno Dello Stato o di un Ente Pubblico o per il Conseguimento di Erogazioni Pubbliche e Frode (Art. 24 D.Lgs. 231/2001)	**Modello Operativo: Truffa in Danno dello Stato o di altro Ente Pubblico (art. 640, II comma, n. 1, c.p.)**
Indebita Percezione di Erogazioni, Truffa In Danno Dello Stato o di un Ente Pubblico o per il Conseguimento di Erogazioni Pubbliche e Frode (Art. 24 D.Lgs. 231/2001)	Modello operativo: Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640 ter c.p.)
Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	Modello Operativo: Falsità in un Documento Informatico Pubblico o Avente Efficacia Probatoria (art. 491-bis c.p.)
Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	Modello Operativo: Accesso Abusivo ad un Sistema Informatico o Telematico (Art. 615-Ter C.P.)
Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	Modello Operativo: Detenzione e Diffusione Abusiva di Codici di Accesso a Sistemi Informatici o Telematici (Art. 615-Quater C.P.)
Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	Modello Operativo: Diffusione di Apparecchiature, Dispositivi o Programmi Informatici Diretti a Danneggiare o Interrompere un Sistema Informatico o Telematico (Art. 615-Quinquies C.P.)
Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	Modello Operativo: Intercettazione, Impedimento o Interruzione Illecita di Comunicazioni Informatiche o Telematiche (art. 617-quater c.p.)
Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	Modello Operativo: Installazione di Apparecchiature atte ad Intercettare, Impedire o Interrompere Comunicazioni Informatiche o Telematiche (art. 617-quinquies c.p.)
Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	Modello operativo: Danneggiamento di Informazioni, Dati e Programmi Informatici (art. 635-bis c.p.)
Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	Modello Operativo: Danneggiamento di Informazioni, Dati e Programmi Informatici Utilizzati dallo Stato o da Altro Ente Pubblico o Comunque di Pubblica Utilità (art. 635-ter c.p.)
Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	Modello Operativo: Danneggiamento di Sistemi Informatici o Telematici (art. 635-quater c.p.)
Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	Modello Operativo: Danneggiamento di Sistemi Informatici o Telematici di Pubblica Utilità (art. 635-quinquies c.p.)
Delitti di Criminalità Organizzata (art. 24 ter D.Lgs. 231/2001)	**Modello Operativo: Associazione per Delinquere (art. 416 c.p.)**

Delitti di Criminalità Organizzata (art. 24 ter D.Lgs. 231/2001)	Modello operativo: Associazione di tipo mafioso (art. 416-bis c.p.)
Delitti di Criminalità Organizzata (art. 24 ter D.Lgs. 231/2001)	Modello operativo: Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al decreto del Presidente della Repubblica 23 gennaio 1973, n. 43)
Delitti di Criminalità Organizzata (art. 24 ter D.Lgs. 231/2001)	Modello operativo: Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309)
Delitti di Criminalità Organizzata (art. 24 ter D.Lgs. 231/2001)	Modello operativo: Illegale fabbricazione, introduzione nello Stato, vendita, detenzione e porto in luogo pubblico di armi da guerra (cfr. art. 407 c.p.p.)
Concussione e corruzione (art. 25 D.Lgs. 231/2001)	Modello operativo: Concussione (art. 317 c.p.)
Concussione e corruzione (art. 25 D.Lgs. 231/2001)	Modello operativo: Corruzione per l'esercizio della funzione (art. 318 c.p.)
Concussione e corruzione (art. 25 D.Lgs. 231/2001)	Modello operativo: Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)
Concussione e corruzione (art. 25 D.Lgs. 231/2001)	Modello operativo: Corruzione in atti giudiziari (art. 319-ter c.p.)
Concussione e corruzione (art. 25 D.Lgs. 231/2001)	Modello operativo: Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)
Concussione e corruzione (art. 25 D.Lgs. 231/2001)	Modello operativo: Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)
Concussione e corruzione (art. 25 D.Lgs. 231/2001)	Modello operativo: Pene per il corruttore (art. 321 c.p.)
Concussione e corruzione (art. 25 D.Lgs. 231/2001)	Modello operativo: Istigazione alla Corruzione (art. 322 c.p.)
Concussione e corruzione (art. 25 D.Lgs. 231/2001)	Modello operativo: Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.)
Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 bis D.Lgs. 231/2001)	Modello operativo: Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)
Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 bis D.Lgs. 231/2001)	Modello operativo: Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)
Reati societari (art. 25 ter D.Lgs. 231/2001)	Modello operativo: False comunicazioni sociali (artt. 2621 e 2621 bis c.c.)
Reati societari (art. 25 ter D.Lgs. 231/2001)	Modello operativo: Impedito controllo (art. 2625, comma 2, c.c.)

Reati societari (art. 25 ter D.Lgs. 231/2001)	Modello operativo: Indebita restituzione di conferimenti (art. 2626 c.c.)
Reati societari (art. 25 ter D.Lgs. 231/2001)	Modello operativo: Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
Reati societari (art. 25 ter D.Lgs. 231/2001)	Modello operativo: Illecite operazioni su azioni o quote sociali o della società controllante (art. 2628 c.c.)
Reati societari (art. 25 ter D.Lgs. 231/2001)	Modello operativo: Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
Reati societari (art. 25 ter D.Lgs. 231/2001)	Modello operativo: Formazione fittizia del capitale (art. 2632 c.c.)
Reati societari (art. 25 ter D.Lgs. 231/2001)	Modello operativo: Corruzione tra privati (art. 2635, comma 3 c.c.)
Delitti contro la personalità individuale (Art. 25-quinquies D.lgs. 231/2001)	Modello operativo: Pornografia minorile (art. 600-ter c.p.) da cancellare - Riserva di valutazione con OdV
Delitti contro la personalità individuale (Art. 25-quinquies D.lgs. 231/2001)	Modello operativo: Detenzione di materiale pornografico (art. 600-quater c.p.) da cancellare - Riserva di valutazione con OdV
Delitti contro la personalità individuale (Art. 25-quinquies D.lgs. 231/2001)	Modello operativo: - Pornografia virtuale (art. 600-quater.1 c.p.) da cancellare - Riserva di valutazione con OdV
Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies D.Lgs. 231/2001)	Modello operativo: Omicidio colposo (art. 589 c.p.)
Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies D.Lgs. 231/2001)	Modello operativo: Lesioni personali colpose (art. 590 c.p.)
Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies D.Lgs. 231/2001)	Modello operativo: Ricettazione (art. 648 c.p.)
Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies D.Lgs. 231/2001)	Modello operativo: Riciclaggio (art. 648-bis c.p.)
Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies D.Lgs. 231/2001)	Modello operativo: Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)
Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies D.Lgs. 231/2001)	Modello operativo: Autoriciclaggio (art. 648-ter.1 c.p.)
Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001) da cancellare - Riserva di valutazione con OdV	Modello operativo: Messa a disposizione del pubblico in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, e senza averne diritto di un'opera o di parte di un'opera dell'ingegno protetta (art. 171, co. 1, lett a-bis e co. 3, L. 633/1941)

Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001)	Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale ovvero concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi di protezione di programmi per elaboratori (art. 171-bis, L. 633/1941)
Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001) da cancellare - Riserva di valutazione con OdV	Reati commessi a fini di lucro, per uso non personale, e caratterizzati da una delle seguenti condotte descritte all'art. 171-ter, comma 1, L. 633/1941
Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001) da cancellare - Riserva di valutazione con OdV	Reati caratterizzati da una delle seguenti condotte descritte all'art. 171-ter, comma 2, L. 633/1941
Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001) da cancellare - Riserva di valutazione con OdV	Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno, da parte di produttori o importatori di tali supporti, ovvero falsa dichiarazione circa l'assolvimento degli obblighi sul contrassegno (art. 171-septies, L. 633/1941)
Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001) da cancellare - Riserva di valutazione con OdV	Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies, L. 633/1941)
Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies D.Lgs. 231/2001)	Modello operativo: Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)
Delitti in materia ambientale (art. 25- undecies D.Lgs. 231/2001)	Modello operativo: Attività di gestione di rifiuti non autorizzata (Art. 256 D. Lgs. 152/2006)
Delitti in materia ambientale (art. 25- undecies D.Lgs. 231/2001)	Modello operativo: Traffico illecito di rifiuti (Art. 259, comma 1 D. Lgs. 152/2006)
Delitti in materia ambientale (art. 25- undecies D.Lgs. 231/2001)	Modello operativo: Attività organizzate per il traffico illecito di rifiuti (Art. 260 D. Lgs. 152/2006)
Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies D.Lgs. 231/2001)	Modello operativo: Art. 22, comma 12 bis, D.Lgs. 25 luglio 1998, n. 286 ("Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero")
Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies D.Lgs. 231/2001)	Modello operativo: Definizione di reato transnazionale (Art. 3 - L. 146/2006)

Per semplicità di descrizione si intende per prevendita le attività di progettazione dell'offerta di vendita, eseguita nelle BU e per postvendita le attività di installazione e manutenzione eseguite nella Direzione Operation

Indebita Percezione di Erogazioni, Truffa In Danno Dello Stato o di un Ente Pubblico o per il Conseguimento di Erogazioni Pubbliche e Frode (Art. 24 D.Lgs. 231/2001)	
Modello Operativo: Truffa in Danno dello Stato o di altro Ente Pubblico (art. 640, II comma, n. 1, c.p.)	
Processo e Responsabilità	▪ Processo di Pre Vendita: gestione iter commerciale per Progettazione di Offerte di Vendita e/o partecipazione e gare pubbliche ▪ Direzione Vendite
Rischio Lordo	ALTO
Procedure in essere	▪ Limiti di firma (per valore economico e per sconto) Workflow del Sistema Informativo aziendale SIM con blocchi automatici al superamento dei limiti di firma dei commerciali per validazione da parte del D.G. o dell'Amministratore Delegato Invio documentazione tramite Posta certificata (PEC) nel rispetto dei poteri di delega conferiti ▪ Caricamento su portali dei Clienti con password dedicate e temporanee, rilasciate e gestite dal cliente (inviate con PEC) ▪ Tracciabilità invii (PEC) ▪ Archivio centralizzato degli invii PEC su cloud ▪ Identificazione e raccolta della documentazione necessaria con il supporto delle funzioni aziendali interessate (archivio Clienti?) ▪ Verifica documentazione ricevuta di concerto con il Funzionario di vendita ▪ Archiviazione di una copia di quanto formalizzato nel Sistema Informativo Maticmind (SIM) all'interno della scheda di lavoro associata (SDL) ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Indebita Percezione di Erogazioni, Truffa In Danno Dello Stato o di un Ente Pubblico o per il Conseguimento di Erogazioni Pubbliche e Frode (Art. 24 D.Lgs. 231/2001)	
Modello operativo: Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640 ter c.p.)	
Processo e Responsabilità	▪ Post Vendita: Erogazione dei servizi di installazione, system integration e assistenza ▪ Post Vendita: sviluppo e manutenzione di applicazioni software ▪ Direzione Operation
Rischio Lordo	MEDIO
Procedure in essere	▪ Valutazione delle competenze tecniche delle risorse ▪ Accesso al Sistema Informatico del Cliente con ID e PW abilitate dal Cliente stesso ▪ Profilazione delle credenziali di accesso definita dal Cliente ▪ Definizione di apposite modalità di comportamento nel caso di accesso alla rete del Cliente parte integrante delle policy aziendali obbligatorie per tutti i dipendenti ▪ Nomina di Amministratori di Sistema con conseguente e formale assunzione di responsabilità e impegno al rispetto delle policy del cliente sia da parte di tecnici interni che di terze parti ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	MEDIO BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	
Modello Operativo: Falsità in un Documento Informatico Pubblico o Avente Efficacia Probatoria (art. 491-bis c.p.)	
Processo e Responsabilità	▪ Processo di Pre Vendita: gestione iter commerciale per progettazione di offerte di vendita e/o partecipazione e gare pubbliche ▪ Direzione Vendita
Rischio Lordo	ALTO
Procedure in essere	▪ Invio documentazione tramite Posta certificata nel rispetto dei poteri di delega conferiti ▪ Identificazione e raccolta della documentazione necessaria con il supporto delle funzioni aziendali interessate ▪ Verifica documentazione ricevuta di concerto con il Funzionario di vendita ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	
Modello Operativo: Accesso Abusivo ad un Sistema Informatico o Telematico (Art. 615 - Ter C.P.)	
Processo e Responsabilità	▪ Processo di Pre Vendita: gestione iter commerciale per Progettazione di Offerte di Vendita e/o partecipazione e gare pubbliche ▪ Direzione Vendite ▪ Processo di Post Vendita - Erogazione dei servizi di installazione, system integration e assistenza ▪ Post Vendita: sviluppo e manutenzione di applicazioni software ▪ Direzione Operation
Rischio Lordo	ALTO
Procedure in essere	▪ Accesso alla rete del cliente con credenziali abilitate dal cliente stesso ▪ Profilazione delle credenziali di accesso definita dal cliente ▪ Gestione con password di servizio che consente il tracciamento degli accessi Maticmind ▪ Definizione di apposite modalità di comportamento nel caso di accesso alla rete del cliente parte integrante delle policy aziendali obbligatorie per tutti i dipendenti ▪ Nomina di Amministratori di Sistema con conseguente e formale assunzione di responsabilità e impegno al rispetto delle policy del cliente sia da parte di tecnici interni che di terze parti ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	
Modello Operativo: Detenzione e Diffusione Abusiva di Codici di Accesso a Sistemi Informatici o Telematici (Art. 615-Quater C.P.)	
Processo e Responsabilità	▪ Processo di Pre Vendita: gestione iter commerciale per Progettazione di Offerte di Vendita e/o partecipazione e gare pubbliche ▪ Direzione Vendite ▪ Processo di Post Vendita - Erogazione dei servizi di installazione, system integration e assistenza oppure di sviluppo e manutenzione di applicazioni software ▪ Direzione Operation
Rischio Lordo	ALTO
Procedure in essere	▪ Accesso alla rete del Cliente con credenziali abilitate dal Cliente stesso ▪ Profilazione delle credenziali di accesso definita dal cliente ▪ Gestione del tracciamento degli accessi Maticmind ▪ Definizione di apposite modalità di comportamento come parte integrante delle policy aziendali obbligatorie per tutti i dipendenti nel caso di accesso alla rete del Cliente ▪ Nomina di Amministratori di Sistema con conseguente e formale assunzione di responsabilità e impegno al rispetto delle policy del cliente sia da parte di tecnici interni che di terze parti ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	
Modello Operativo: Diffusione di Apparecchiature, Dispositivi o Programmi Informatici Diretti a Danneggiare o Interrompere un Sistema Informatico o Telematico (Art. 615-Quinquies C.P.)	
Processo e Responsabilità	▪ Direzione Vendite ▪ Processo di Post Vendita: Erogazione dei servizi di installazione, system integration e assistenza ▪ Processo di Post Vendita: sviluppo e manutenzione di applicazioni software ▪ Direzione Operation
Rischio Lordo	ALTO
Procedure in essere	▪ Accesso alla rete del Cliente con credenziali abilitate dal Cliente stesso ▪ Profilazione delle Credenziali di Accesso definita dal Cliente ▪ Gestione del tracciamento degli accessi Maticmind alle sedi ed ai sistemi del Cliente ▪ Definizione di apposite modalità di comportamento come parte integrante delle policy aziendali obbligatorie per tutti i dipendenti nel caso di accesso alla rete del Cliente ▪ Controllo da parte del responsabile delle attività operative da parte Cliente di quanto effettuato dai tecnici e/o fornitori ▪ Approvazione dell'esito delle attività operative da parte del Cliente (MIT o Verbale di Collaudo -> da implementare al riguardo) ▪ Nomina di Amministratori di Sistema con conseguente e formale assunzione di responsabilità e impegno al rispetto delle policy del cliente sia da parte di tecnici interni che di terze parti ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	
Modello Operativo: Intercettazione, Impedimento o Interruzione Illecita di Comunicazioni Informatiche o Telematiche (art. 617-quater c.p.)	
Processo e Responsabilità	▪ Direzione Vendite ▪ Processo di Post Vendita - Erogazione dei servizi di installazione, system integration e assistenza ▪ Post Vendita: sviluppo e manutenzione di applicazioni software ▪ Direzione Operation
Rischio Lordo	MEDIO
Procedure in essere	▪ Accesso alla rete del Cliente con credenziali abilitate dal Cliente stesso ▪ Profilazione delle credenziali di accesso definita dal Cliente ▪ Gestione del tracciamento degli accessi Maticmind nelle sedi e ai sistemi del Cliente ▪ Definizione di apposite modalità di comportamento come parte integrante delle policy aziendali obbligatorie per tutti i dipendenti nel caso di accesso alla rete del Cliente ▪ Controllo da parte del responsabile del Cliente delle attività operative di quanto effettuato dai tecnici e/o fornitori ▪ Approvazione dell'esito delle attività operative da parte del Cliente (MIT o Verbale di Collaudo -> da implementare al riguardo) ▪ Nomina di Amministratori di Sistema con conseguente e formale assunzione di responsabilità e impegno al rispetto delle policy del cliente sia da parte di tecnici interni che di terze parti ▪ ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	
Modello Operativo: Installazione di Apparecchiature atte ad Intercettare, Impedire o Interrompere Comunicazioni Informatiche o Telematiche (art. 617-quinquies c.p.)	
Processo e Responsabilità	▪ Direzione Vendite ▪ Processo di Post Vendita - Erogazione dei servizi di installazione, system integration e assistenza ▪ Post Vendita: sviluppo e manutenzione di applicazioni software ▪ Direzione Operation
Rischio Lordo	MEDIO
Procedure in essere	▪ Accesso alla rete del Cliente con credenziali abilitate dal Cliente stesso ▪ Profilazione delle credenziali di accesso definita dal Cliente ▪ Gestione del tracciamento degli accessi Maticmind alla sede ed ai sistemi del Cliente ▪ Definizione di apposite modalità di comportamento nel caso di accesso alla rete del Cliente parte integrante delle policy aziendali obbligatorie per tutti i dipendenti ▪ Controllo da parte del responsabile del Cliente delle attività operative di quanto effettuato dai tecnici e/o fornitori ▪ Approvazione dell'esito delle attività operative da parte del Cliente (MIT o Verbale di Collaudo -> da implementare al riguardo) ▪ Nomina di Amministratori di Sistema con conseguente e formale assunzione di responsabilità e impegno al rispetto delle policy del cliente sia da parte di tecnici interni che di terze parti ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	
Modello operativo: Danneggiamento di Informazioni, Dati e Programmi Informatici (art. 635-bis c.p.)	
Processo e Responsabilità	▪ Processo di Post Vendita: Erogazione dei servizi di installazione, system integration e assistenza ▪ Post Vendita: sviluppo e manutenzione di applicazioni software ▪ Direzione Operation ▪ Direzione Vendite
Rischio Lordo	ALTO
Procedure in essere	▪ Accesso alla rete del Cliente con credenziali abilitate dal Cliente stesso ▪ Profilazione delle credenziali di accesso definita dal Cliente ▪ Gestione del tracciamento degli accessi Maticmind alla sede ed ai sistemi del Cliente ▪ Definizione di apposite modalità di comportamento come parte integrante delle policy aziendali obbligatorie per tutti i dipendenti nel caso di accesso alla rete del cliente ▪ Controllo da parte del responsabile del Cliente delle attività operative di quanto effettuato dai tecnici e/o fornitori ▪ Approvazione dell'esito delle attività operative da parte del Cliente (MIT o Verbale di Collaudo -> da implementare al riguardo) ▪ Nomina di Amministratori di Sistema con conseguente e formale assunzione di responsabilità e impegno al rispetto delle policy del Cliente sia da parte di tecnici interni che di terze parti ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	
Modello Operativo: Danneggiamento di Informazioni, Dati e Programmi Informatici Utilizzati dallo Stato o da Altro Ente Pubblico o Comunque di Pubblica Utilità (art. 635-ter c.p.)	
Processo e Responsabilità	▪ Processo di Post Vendita - Erogazione dei servizi di installazione, system integration e assistenza ▪ Post Vendita: sviluppo e manutenzione di applicazioni software ▪ Direzione Operation ▪ Direzione Vendite
Rischio Lordo	ALTO
Procedure in essere	▪ Accesso alla rete del Cliente con credenziali abilitate dal Cliente stesso ▪ Profilazione delle credenziali di accesso definita dal Cliente ▪ Gestione del tracciamento degli accessi Maticmind alla sede ed ai sistemi del Cliente ▪ Definizione di apposite modalità di comportamento come parte integrante delle policy aziendali obbligatorie per tutti i dipendenti nel caso di accesso alla rete del Cliente ▪ Controllo da parte del responsabile del Cliente delle attività operative di quanto effettuato dai tecnici e/o fornitori ▪ Approvazione dell'esito delle attività operative da parte del Cliente (MIT o Verbale di Collaudo -> da implementare al riguardo) ▪ Nomina di Amministratori di Sistema con conseguente e formale assunzione di responsabilità e impegno al rispetto delle policy del cliente sia da parte di tecnici interni che di terze parti ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	
Modello Operativo: Danneggiamento di Sistemi Informatici o Telematici (art. 635-quater c.p.)	
Processo e Responsabilità	▪ Processo di Post Vendita: Erogazione dei servizi di installazione, system integration e assistenza ▪ Post Vendita: sviluppo e manutenzione di applicazioni software ▪ Direzione Operation ▪ Direzione Vendite
Rischio Lordo	ALTO
Procedure in essere	▪ Accesso alla rete del Cliente con credenziali abilitate dal Cliente stesso ▪ Profilazione delle credenziali di accesso definita dal Cliente ▪ Gestione del tracciamento degli accessi Maticmind alla sede ed ai sistemi del Cliente ▪ Definizione di apposite modalità di comportamento come parte integrante delle policy aziendali obbligatorie per tutti i dipendenti nel caso di accesso alla rete del Cliente ▪ Controllo da parte del responsabile del Cliente delle attività operative di quanto effettuato dai tecnici e/o fornitori ▪ Approvazione dell'esito delle attività operative da parte del Cliente (MIT o Verbale di Collaudo -> da implementare al riguardo) ▪ Nomina di Amministratori di Sistema con conseguente e formale assunzione di responsabilità e impegno al rispetto delle policy del cliente sia da parte di tecnici interni che di terze parti ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti informatici e trattamento illecito di dati (art. 24 bis D.Lgs. 231/2001)	
Modello Operativo: Danneggiamento di Sistemi Informatici o Telematici di Pubblica Utilità (art. 635-quinquies c.p.)	
Processo e Responsabilità	▪ Processo di Post Vendita: Erogazione dei servizi di installazione, system integration e assistenza ▪ Post Vendita: sviluppo e manutenzione di applicazioni software ▪ Direzione Operation ▪ Direzione Vendite
Rischio Lordo	ALTO
Procedure in essere	▪ Accesso alla rete del Cliente con credenziali abilitate dal Cliente stesso ▪ Profilazione delle credenziali di accesso definita dal Cliente ▪ Gestione del tracciamento degli accessi Maticmind alla sede ed ai sistemi del Cliente ▪ Definizione di apposite modalità di comportamento come parte integrante delle policy aziendali obbligatorie per tutti i dipendenti nel caso di accesso alla rete del cliente ▪ Controllo da parte del responsabile del Cliente delle attività operative di quanto effettuato dai tecnici e/o fornitori ▪ Approvazione dell'esito delle attività operative da parte del Cliente (MIT o Verbale di Collaudo -> da implementare al riguardo) ▪ Nomina di Amministratori di Sistema con conseguente e formale assunzione di responsabilità e impegno al rispetto delle policy del cliente sia da parte di tecnici interni che di terze parti ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti di Criminalità Organizzata (art. 24 ter D.Lgs. 231/2001)	
Modello Operativo: Associazione per Delinquere (art. 416 c.p.)	
Processo e Responsabilità	▪ Costituzione RTI per partecipazione a gare ▪ Direzione Vendite ▪ Direzione Vendite Acquisti di beni e servizi da/presso terze parti ▪ Direzione Acquisti
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Attività gestita prevalentemente tramite Carrier ▪ RTI con Carrier noti ▪ Autonomia nulla dei singoli funzionari di vendita su raggruppamenti o business particolari, i quali sono definiti dalla Direzione Vendite ▪ Accordi firmati dai Procuratori ▪ Workflow del Sistema Informativo aziendale SIM con blocchi automatici al superamento dei limiti di firma per validazione da parte del D.G. o dell'Amministratore Delegato ▪ Invio documentazione tramite Posta certificata (PEC) nel rispetto dei poteri di delega conferiti ▪ Tracciabilità invii (PEC) ▪ Archiviazione di una copia di quanto formalizzato nel Sistema Informativo Maticmind (Navision) in riferimento alla Commessa e SDL di riferimento ▪ Accordi Quadro formalizzati con i fornitori e/o Terze Parti ▪ Verifiche inerenti bilanci, carichi penali, visure camerali, ecc. su potenziali nuovi partner da parte della Direzione Amministrativa ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti di Criminalità Organizzata (art. 24 ter D.Lgs. 231/2001)	
Modello operativo: Associazione di tipo mafioso (art. 416-bis c.p.)	
Processo e Responsabilità	▪ Costituzione RTI per partecipazione a gare ▪ Direzione Vendite ▪ Direzione Vendite Acquisti di beni e servizi da/presso terze parti ▪ Direzione Acquisti
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Attività gestita prevalentemente tramite Carrier ▪ RTI con Carrier noti ▪ Autonomia nulla dei singoli funzionari di vendita su raggruppamenti o business particolari, i quali sono definiti dalla Direzione Vendite ▪ Accordi firmati dai Procuratori ▪ Workflow del Sistema Informativo aziendale SIM con blocchi automatici al superamento dei limiti di firma per validazione da parte del D.G. o dell'Amministratore Delegato ▪ Invio documentazione tramite Posta certificata (PEC) nel rispetto dei poteri di delega conferiti ▪ Tracciabilità invii (PEC) ▪ Archiviazione di una copia di quanto formalizzato nel Sistema Informativo Maticmind (Navision) in riferimento alla Commessa e SDL di riferimento ▪ Accordi Quadro formalizzati con i fornitori e/o Terze Parti ▪ Verifiche inerenti bilanci, carichi penali, visure camerali, ecc. su potenziali nuovi partner da parte della Direzione Amministrativa ▪ Verifiche da parte della Direzione Amministrativa e Direzione Gestione Controllo e Reporting ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti di Criminalità Organizzata (art. 24 ter D.Lgs. 231/2001)	
Modello operativo: Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al decreto del Presidente della Repubblica 23 gennaio 1973, n. 43)	
Processo e Responsabilità	▪ Acquisti di beni e servizi da/presso terze parti ▪ Direzione Acquisti
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Fornitori qualificati nel Repository Albo Fornitori ▪ Rispetto iter di qualifica e valutazione dei fornitori/Carrier ▪ Acquisto diretto da fornitori italiani/vendor ▪ Acquisiti legati a specifico ordine/commessa/SDL o relativi ad una Richiesta di Acquisto (RdA) ▪ Controllo corrispondenza Offerta-Ordine di Vendita e Ordine di Acquisto ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale (Navision) che in relazione al valore economico e alla tipologia è inoltrata ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Solo le RdA autorizzate possono originare reali esigenze di approvvigionamento ▪ Ordine Cliente abbinato ad articoli e prezzi definito con il fornitore in fase commerciale ▪ Ordine a fornitore fatto con il Sistema Informativo aziendale attraverso la trasformazione automatica dello stesso dell'Ordine del Cliente. ▪ Controlli in accettazione (Ordine - bolla - merce) ▪ Corrieri in consegna definito dal fornitore ▪ Verifiche da parte della Direzione Amministrativa e Direzione Gestione Controllo e Reporting ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti di Criminalità Organizzata (art. 24 ter D.Lgs. 231/2001)	
Modello operativo: Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309)	
Processo e Responsabilità	▪ Acquisti di beni e servizi da/presso terze parti ▪ Direzione Acquisti
Livello di rischio Lordo	BASSO
Procedure in essere	▪ Fornitori qualificati nel Repository Albo Fornitori ▪ Rispetto iter di qualifica e valutazione dei fornitori/Carrier ▪ Acquisto diretto da fornitori italiani/vendor ▪ ▪ Acquisiti legati a specifico ordine/commessa/SDL o relativi ad una Richiesta di Acquisto (RdA) ▪ Controllo corrispondenza Offerta-Ordine ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale (Navision) che in relazione al valore economico e alla tipologia è inoltrata ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Solo le RdA autorizzate possono originare reali esigenze di approvvigionamento ▪ Ordine Cliente abbinato ad articoli e prezzi definito con il fornitore in fase commerciale ▪ Ordine a fornitore fatto con il Sistema Informativo aziendale attraverso la trasformazione automatica dello stesso dell'ordine del Cliente. ▪ Controlli in accettazione (Ordine - bolla - merce) ▪ Corrieri in consegna definito dal fornitore ▪ Verifiche da parte della Direzione Amministrativa e Direzione Gestione Controllo e Reporting ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti di Criminalità Organizzata (art. 24 ter D.Lgs. 231/2001)	
Modello operativo: Illegale fabbricazione, introduzione nello Stato, vendita, detenzione e porto in luogo pubblico di armi da guerra (cfr. art. 407 c.p.p.)	
Processo e Responsabilità	▪ Acquisti di beni e servizi da/presso terze parti ▪ Direzione Acquisti
Livello di rischio Lordo	BASSO
Procedure in essere	▪ Fornitori qualificati nel Repository Albo Fornitori ▪ Stipula Accordi Quadro con Fornitori ▪ Acquisto diretto da fornitori italiani/vendor ▪ Rispetto iter di qualifica e valutazione dei fornitori/Carrier ▪ Acquisiti legati a specifico ordine/commessa/SDL o relativi ad una Richiesta di Acquisto (RdA) ▪ Controllo corrispondenza Offerta-Ordine ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale (Navision) che in relazione al valore economico e alla tipologia è inoltrata ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Solo le RdA autorizzate possono originare reali esigenze di approvvigionamento ▪ Ordine cliente abbinato ad articoli e prezzi definito con il fornitore in fase commerciale ▪ Ordine a fornitore fatto con il Sistema Informativo aziendale attraverso la trasformazione automatica dello stesso dell'ordine del cliente. ▪ Controlli in accettazione (Ordine - bolla - merce) ▪ Corrieri in consegna definito dal fornitore ▪ Verifiche da parte della Direzione Amministrativa e Direzione Gestione Controllo e Reporting ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Concussione (art. 317 c.p.)	
Processo e Responsabilità	▪ Pre Vendita e Vendita ▪ Direzione Vendite ▪ Direzione Operation
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Controllo di congruità delle fatture per i servizi erogati: da parte della funzione interna (Acquisti) controllo di corrispondenza tra la fattura relativa al servizio erogato (sigla fattura e mail) con Ordine fornitore (Ordine Cliente/RdA - Ordine Fornitore - Fattura) ▪ Carte di credito assegnate alla Direzione Vendite con rendicontazione mensile ▪ Compilazione mensile di una nota spese per gli acquisti effettuati con carta di credito in dotazione approvata dal proprio responsabile ▪ Controllo note spese - giustificativi ▪ ▪ Definizione poteri di firma degli amministratori ▪ Individuazione di partner per RTI nell'ambito della Funzione Vendite con il supporto dell'Ufficio Legale esterno incaricato ▪ Acquisto prodotti e/o servizi da terzi solo in funzione dei uno specifico Ordine Cliente ▪ Acquisiti legati a specifico ordine/commessa o a una Richiesta di Acquisto (RdA) ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale (Navision) che in relazione al valore economico e alla tipologia la inoltra ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Esigenze di approvvigionamento determinate esclusivamente da RdA autorizzate ▪ ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciamento degli acquisti effettuati degli Ordini (destinati alla vendita) e delle RdA sul Sistema Informativo Aziendale SIM e Navision ▪ ▪ Accordi Quadro con listini e sconti previsti relativamente a Vendor - Cliente - Maticmind ▪ Approvazioni a più livelli in base all'entità dell'ordine ▪ ▪ Autorizzazione alle trasferte è preventivamente richiesta via mail al proprio responsabile e dallo stesso ottenuta tramite il Sistema Informativo aziendale ▪ prenotazioni degli alberghi e all'acquisto dei titoli di viaggio secondo i criteri definiti da Risorse Umane previa autorizzazione ▪ trasferte all'estero effettuate esclusivamente se autorizzate dalla Direzione ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare ▪
Rischio Residuo	BASSO

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Corruzione per l'esercizio della funzione (art. 318 c.p.)	
Processo e Responsabilità	▪ Pre Vendita e Vendita ▪ Direzione Vendite ▪ Gestione adempimenti normativi SSL ▪ Direzione Acquisti (Responsabile Salute & Sicurezza) ▪
Livello di rischio Lordo	ALTO
Procedure in essere	▪ ▪ Controllo di congruità delle fatture per i servizi erogati: da parte della funzione interna (Acquisti) controllo di corrispondenza tra la fattura relativa al servizio erogato (sigla fattura e mail) con Ordine fornitore (Ordine Cliente/RdA - Ordine Fornitore - Fattura) ▪ Carte di credito assegnate alla Direzione Vendite con rendicontazione mensile ▪ Compilazione mensile di una nota spese per gli acquisti effettuati con carta di credito in dotazione approvata dal proprio responsabile ▪ Controllo note spese - giustificativi ▪ ▪ Definizione poteri di firma degli amministratori ▪ Individuazione di partner per RTI nell'ambito della Funzione Vendite con il supporto dell'Ufficio Legale esterno incaricato ▪ Acquisto prodotti e/o servizi da terzi solo in funzione dei uno specifico Ordine Cliente ▪ Acquisiti legati a specifico ordine/commessa o a una Richiesta di Acquisto (RdA) ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale (Navision) che in relazione al valore economico e alla tipologia la inoltra ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Esigenze di approvvigionamento determinate esclusivamente da RdA autorizzate ▪ ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciamento degli acquisti effettuati degli Ordini (destinati alla vendita) e delle RdA sul Sistema Informativo Aziendale SIM e Navision ▪ ▪ Accordi Quadro con listini e sconti previsti relativamente a Vendor - Cliente - Maticmind ▪ Approvazioni a più livelli in base all'entità dell'ordine ▪ ▪ Autorizzazione alle trasferte è preventivamente richiesta via mail al proprio responsabile e dallo stesso ottenuta tramite il Sistema Informativo aziendale ▪ prenotazioni degli alberghi e all'acquisto dei titoli di viaggio secondo i criteri definiti da Risorse Umane previa autorizzazione ▪ trasferte all'estero effettuate esclusivamente se autorizzate dalla Direzione ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare ▪

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Corruzione per l'esercizio della funzione (art. 318 c.p.)	
Rischio Residuo	BASSO

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.)	
Processo e Responsabilità	▪ Direzione Vendite ▪ Pre Vendita e Vendita ▪ Direzione Vendite
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Controllo di congruità delle fatture per i servizi erogati: da parte della funzione interna (Acquisti) controllo di corrispondenza tra la fattura relativa al servizio erogato (sigla fattura e mail) con Ordine fornitore (Ordine Cliente/RdA - Ordine Fornitore - Fattura) ▪ Carte di credito assegnate alla Direzione Vendite con rendicontazione mensile ▪ Compilazione mensile di una nota spese per gli acquisti effettuati con carta di credito in dotazione approvata dal proprio responsabile ▪ Controllo note spese - giustificativi ▪ ▪ Definizione poteri di firma degli amministratori ▪ Individuazione di partner per RTI nell'ambito della Funzione Vendite con il supporto dell'Ufficio Legale esterno incaricato ▪ Acquisto prodotti e/o servizi da terzi solo in funzione dei uno specifico Ordine Cliente ▪ Acquisiti legati a specifico ordine/commessa o a una Richiesta di Acquisto (RdA) ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale (Navision) che in relazione al valore economico e alla tipologia la inoltra ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Esigenze di approvvigionamento determinate esclusivamente da RdA autorizzate ▪ ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciamento degli acquisti effettuati degli Ordini (destinati alla vendita) e delle RdA sul Sistema Informativo Aziendale SIM e Navision ▪ ▪ Accordi Quadro con listini e sconti previsti relativamente a Vendor - Cliente - Maticmind ▪ Approvazioni a più livelli in base all'entità dell'ordine ▪ ▪ Autorizzazione alle trasferte è preventivamente richiesta via mail al proprio responsabile e dallo stesso ottenuta tramite il Sistema Informativo aziendale ▪ prenotazioni degli alberghi e all'acquisto dei titoli di viaggio secondo i criteri definiti da Risorse Umane previa autorizzazione ▪ trasferte all'estero effettuate esclusivamente se autorizzate dalla Direzione ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare ▪
Rischio Residuo	BASSO

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Corruzione in atti giudiziari (art. 319-ter c.p.)	
Processo e Responsabilità	▪ Pre Vendita, Post Vendita ▪ Direzione Vendite ▪ Direzione Acquisti ▪ Gestione adempimenti normativi ▪ Direzione Amministrativa ▪ Direzione Acquisti ▪ Direzione Acquisti (Responsabile Salute & Sicurezza SSL)
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Controllo congruità fatture per servizi: controllo con Funzione interna che ha usufruito dei servizi per effettuazione reale delle attività di cui alle (sigla fattura e mail) - controllo congruità con ordine fornitore (ordine cliente/RdA - ordine fornitore - fattura) ▪ Carte di credito con rendicontazione mensile ▪ Compilazione mensile di una nota spese per gli acquisti effettuati con carta di credito in dotazione approvata dal proprio responsabile ▪ Controllo note spese - giustificativi ▪ Definizione poteri di firma degli amministratori ▪ Acquisto servizi da terzi solo in funzione dei uno specifico Ordine Cliente ▪ Possibilità di effettuare acquisiti di beni e servizi destinati ICT solo tramite Richiesta di Acquisto (RdA) o previa stipula da parte della Direzione di specifici Contratti ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale che in relazione al valore economico e alla tipologia la inoltra ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Solo le RdA autorizzate possono originare reali esigenze di approvvigionamento ▪ Gestione parco macchine: Richiesta acquisto a Ufficio Acquisti ▪ Gestione cellulari aziendali: richiesta acquisto a Ufficio Acquisti ▪ Richiesta e ottenimento dal dipendente assegnatario della firma per ricezione auto/cellulare ▪ Acquisto diretto da fornitori ▪ Acquisiti legati a specifico ordine/commessa o a una Richiesta di Acquisto (RdA) ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ Ordine a fornitore fatto con il Sistema Informativo aziendale attraverso la trasformazione automatica dell'Ordine Cliente ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciabilità su il Sistema Informativo aziendale di tutti gli ordini (destinati alla vendita) e delle RdA ▪ Accordi quadro con listini e sconti previsti relativamente a Vendor - Cliente - Maticmind ▪ Approvazioni a più livelli in base all'entità dell'ordine ▪ Definizione poteri di firma dei referenti dell'Ufficio Acquisiti ▪ ▪ L'autorizzazione alle trasferte è preventivamente richiesta via mail al proprio responsabile e dallo stesso ottenuta tramite il Sistema Informativo aziendale ▪ Previa autorizzazione, le segreterie provvedono alle prenotazioni degli alberghi e all'acquisto dei titoli di viaggio secondo i criteri definiti da Risorse Umane ▪ Le trasferte all'estero occorre sono richieste tramite apposito modulo e autorizzate dalla Direzione

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Corruzione in atti giudiziari (art. 319-ter c.p.)	
	▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare ▪
Rischio Residuo	BASSO

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)	
Processo e Responsabilità	▪ Pre Vendita e Vendita ▪ Direzione Vendite
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Controllo di congruità delle fatture per i servizi erogati: da parte della funzione interna (Acquisti) controllo di corrispondenza tra la fattura relativa al servizio erogato (sigla fattura e mail) con Ordine fornitore (Ordine Cliente/RdA - Ordine Fornitore - Fattura) ▪ Carte di credito assegnate alla Direzione Vendite con rendicontazione mensile ▪ Compilazione mensile di una nota spese per gli acquisti effettuati con carta di credito in dotazione approvata dal proprio responsabile ▪ Controllo note spese - giustificativi ▪ Definizione poteri di firma degli amministratori ▪ Individuazione di partner per RTI nell'ambito della Funzione Vendite con il supporto dell'Ufficio Legale esterno incaricato ▪ Acquisto prodotti e/o servizi da terzi solo in funzione dei uno specifico Ordine Cliente ▪ Acquisiti legati a specifico ordine/commessa o a una Richiesta di Acquisto (RdA) ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale (Navision) che in relazione al valore economico e alla tipologia la inoltra ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Esigenze di approvvigionamento determinate esclusivamente da RdA autorizzate ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciamento degli acquisti effettuati degli Ordini (destinati alla vendita) e delle RdA sul Sistema Informativo Aziendale SIM e Navision ▪ Accordi Quadro con listini e sconti previsti relativamente a Vendor - Cliente - Maticmind ▪ Approvazioni a più livelli in base all'entità dell'ordine ▪ Autorizzazione alle trasferte è preventivamente richiesta via mail al proprio responsabile e dallo stesso ottenuta tramite il Sistema Informativo aziendale ▪ prenotazioni degli alberghi e all'acquisto dei titoli di viaggio secondo i criteri definiti da Risorse Umane previa autorizzazione ▪ trasferte all'estero effettuate esclusivamente se autorizzate dalla Direzione ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codice Etico e disciplinare
Rischio Residuo	BASSO

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)	
Processo e Responsabilità	▪ Pre Vendita e Vendita ▪ Direzione Vendite ▪ Gestione adempimenti normativi SSL ▪ Direzione Acquisti (Responsabile Salute & Sicurezza)
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Controllo di congruità delle fatture per i servizi erogati: da parte della funzione interna (Acquisti) controllo di corrispondenza tra la fattura relativa al servizio erogato (sigla fattura e mail) con Ordine fornitore (Ordine Cliente/RdA - Ordine Fornitore - Fattura) ▪ Carte di credito assegnate alla Direzione Vendite con rendicontazione mensile ▪ Compilazione mensile di una nota spese per gli acquisti effettuati con carta di credito in dotazione approvata dal proprio responsabile ▪ Controllo note spese - giustificativi ▪ Definizione poteri di firma degli amministratori ▪ Individuazione di partner per RTI nell'ambito della Funzione Vendite con il supporto dell'Ufficio Legale esterno incaricato ▪ Acquisto prodotti e/o servizi da terzi solo in funzione dei uno specifico Ordine Cliente ▪ Acquisiti legati a specifico ordine/commessa o a una Richiesta di Acquisto (RdA) ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale (Navision) che in relazione al valore economico e alla tipologia la inoltra ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Esigenze di approvvigionamento determinate esclusivamente da RdA autorizzate ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciamento degli acquisti effettuati degli Ordini (destinati alla vendita) e delle RdA sul Sistema Informativo Aziendale SIM e Navision ▪ Accordi Quadro con listini e sconti previsti relativamente a Vendor - Cliente - Maticmind ▪ Approvazioni a più livelli in base all'entità dell'ordine ▪ Autorizzazione alle trasferte è preventivamente richiesta via mail al proprio responsabile e dallo stesso ottenuta tramite il Sistema Informativo aziendale ▪ prenotazioni degli alberghi e all'acquisto dei titoli di viaggio secondo i criteri definiti da Risorse Umane previa autorizzazione ▪ trasferte all'estero effettuate esclusivamente se autorizzate dalla Direzione ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Pene per il corruttore (art. 321 c.p.)	
Processo e Responsabilità	▪ Pre Vendita e Post Vendita ▪ Direzione Vendite ▪ Direzione Acquisti ▪ Gestione adempimenti normativi ▪ Direzione Amministrativa ▪ Direzione Acquisti (Responsabile Salute & Sicurezza SSL)
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Controllo congruità fatture per servizi: controllo con Funzione interna che ha usufruito dei servizi per effettuazione reale delle attività di cui alle (sigla fattura e mail) - controllo congruità con Ordine Fornitore (ordine cliente/RdA - ordine fornitore - fattura) ▪ Carte di credito con rendicontazione mensile ▪ Compilazione mensile di una nota spese per gli acquisti effettuati con carta di credito in dotazione approvata dal proprio responsabile ▪ Controllo note spese - giustificativi ▪ Definizione poteri di firma degli amministratori ▪ Individuazione di partner per RTI nell'ambito della Funzione Vendite con il supporto dell'Ufficio Legale esterno incaricato ▪ Definizione poteri di firma dei funzionari di vendita ▪ Acquisto servizi da terzi solo in funzione dei uno specifico Ordine Cliente ▪ Possibilità di effettuare acquisiti di beni e servizi destinati ICT solo tramite Richiesta di Acquisto (RdA) o previa stipula da parte della Direzione di specifici Contratti ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale che in relazione al valore economico e alla tipologia la inoltra ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Solo le RdA autorizzate possono originare reali esigenze di approvvigionamento ▪ Gestione parco macchine: Richiesta acquisto a Ufficio Acquisti ▪ Gestione cellulari aziendali: richiesta acquisto a Ufficio Acquisti ▪ Richiesta e ottenimento dal dipendente assegnatario della firma per ricezione auto/cellulare ▪ Acquisto diretto da fornitori ▪ Acquisiti legati a specifico ordine/commessa o a una Richiesta di Acquisto (RdA) ▪ Ordine a fornitore fatto con il Sistema Informativo aziendale attraverso la trasformazione automatica dell'ordine cliente ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciabilità sul Sistema Informativo aziendale di tutti gli ordini (destinati alla vendita) e delle RdA ▪ Accordi quadro con listini e sconti previsti relativamente a Vendor - Cliente - Maticmind ▪ Approvazioni a più livelli in base all'entità dell'ordine ▪ Definizione poteri di firma dei referenti dell'Ufficio Acquisiti ▪ L'autorizzazione alle trasferte è preventivamente richiesta via mail al proprio responsabile e dallo stesso ottenuta tramite il Sistema Informativo aziendale ▪ Previa autorizzazione, le segreterie provvedono alle prenotazioni degli alberghi e all'acquisto dei titoli di viaggio secondo i criteri definiti da Risorse Umane ▪ Le trasferte all'estero richieste tramite apposito modulo e autorizzate dalla Direzione

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Pene per il corruttore (art. 321 c.p.)	
	▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Istigazione alla Corruzione (art. 322 c.p.)	
Processo e Responsabilità	▪ Pre Vendita e Vendita ▪ Direzione Vendite ▪
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Controllo di congruità delle fatture per i servizi erogati: da parte della funzione interna (Acquisti) controllo di corrispondenza tra la fattura relativa al servizio erogato (sigla fattura e mail) con Ordine fornitore (Ordine Cliente/RdA - Ordine Fornitore - Fattura) ▪ Carte di credito assegnate alla Direzione Vendite con rendicontazione mensile ▪ Compilazione mensile di una nota spese per gli acquisti effettuati con carta di credito in dotazione approvata dal proprio responsabile ▪ Controllo note spese - giustificativi ▪ ▪ Definizione poteri di firma degli amministratori ▪ Individuazione di partner per RTI nell'ambito della Funzione Vendite con il supporto dell'Ufficio Legale esterno incaricato ▪ Acquisto prodotti e/o servizi da terzi solo in funzione dei uno specifico Ordine Cliente ▪ Acquisiti legati a specifico ordine/commessa o a una Richiesta di Acquisto (RdA) ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale (Navision) che in relazione al valore economico e alla tipologia la inoltra ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Esigenze di approvvigionamento determinate esclusivamente da RdA autorizzate ▪ ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciamento degli acquisti effettuati degli Ordini (destinati alla vendita) e delle RdA sul Sistema Informativo Aziendale SIM e Navision ▪ ▪ Accordi Quadro con listini e sconti previsti relativamente a Vendor - Cliente - Maticmind ▪ Approvazioni a più livelli in base all'entità dell'ordine ▪

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Istigazione alla Corruzione (art. 322 c.p.)	
	▪ Autorizzazione alle trasferte è preventivamente richiesta via mail al proprio responsabile e dallo stesso ottenuta tramite il Sistema Informativo aziendale ▪ prenotazioni degli alberghi e all'acquisto dei titoli di viaggio secondo i criteri definiti da Risorse Umane previa autorizzazione ▪ trasferte all'estero effettuate esclusivamente se autorizzate dalla Direzione ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Concussione e corruzione (art. 25 D.Lgs. 231/2001)	
Modello operativo: Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.)	
Processo e Responsabilità	▪ Pre Vendita e Vendita ▪ Direzione Vendite ▪
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Controllo di congruità delle fatture per i servizi erogati: da parte della funzione interna (Acquisti) controllo di corrispondenza tra la fattura relativa al servizio erogato (sigla fattura e mail) con Ordine fornitore (Ordine Cliente/RdA - Ordine Fornitore - Fattura) ▪ Carte di credito assegnate alla Direzione Vendite con rendicontazione mensile ▪ Compilazione mensile di una nota spese per gli acquisti effettuati con carta di credito in dotazione approvata dal proprio responsabile ▪ Controllo note spese - giustificativi ▪ ▪ Definizione poteri di firma degli amministratori ▪ Individuazione di partner per RTI nell'ambito della Funzione Vendite con il supporto dell'Ufficio Legale esterno incaricato ▪ Acquisto prodotti e/o servizi da terzi solo in funzione dei uno specifico Ordine Cliente ▪ Acquisiti legati a specifico ordine/commessa o a una Richiesta di Acquisto (RdA) ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale (Navision) che in relazione al valore economico e alla tipologia la inoltra ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Esigenze di approvvigionamento determinate esclusivamente da RdA autorizzate ▪ ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciamento degli acquisti effettuati degli Ordini (destinati alla vendita) e delle RdA sul Sistema Informativo Aziendale SIM e Navision ▪ ▪ Accordi Quadro con listini e sconti previsti relativamente a Vendor - Cliente - Maticmind ▪ Approvazioni a più livelli in base all'entità dell'ordine ▪ ▪ Autorizzazione alle trasferte è preventivamente richiesta via mail al proprio responsabile e dallo stesso ottenuta tramite il Sistema Informativo aziendale ▪ prenotazioni degli alberghi e all'acquisto dei titoli di viaggio secondo i criteri definiti da Risorse Umane previa autorizzazione ▪ trasferte all'estero effettuate esclusivamente se autorizzate dalla Direzione ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 bis D.Lgs. 231/2001)	
Modello operativo: Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)	
Processo e Responsabilità	▪ Pre Vendita e Post Vendita ▪ Fornitura Materiali, Delivery e Assistance ▪ Direzione Commerciale ▪ Direzione Operation ▪ Direzione Acquisti
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Acquisito diretto da Vendor ▪ Controllo diretto del Fornitore sul Cliente finale destinatario dei prodotti ▪ Tracciatura seriali dal Vendor ▪ MRA solo su originali tracciati con seriale ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare ▪
Rischio Residuo	BASSO

Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 bis D.Lgs. 231/2001)	
Modello operativo: Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)	
Processo e Rresponsabilità	▪ Pre Vendita e Post Vendita ▪ Fornitura Materiali, Delivery e Assistance ▪ Direzione Vendite ▪ Direzione Operation ▪ Direzione Acquisti
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Acquisito diretto da Vendor ▪ Controllo diretto del Fornitore sul Cliente finale destinatario dei prodotti ▪ Tracciatura seriali dal Vendor ▪ MRA solo su originali tracciati con seriale ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Reati societari (art. 25 ter D.Lgs. 231/2001)	
Modello operativo: False comunicazioni sociali (artt. 2621 e 2621 bis c.c.)	
Processo e Responsabilità	▪ Gestione della Contabilità e Trasposizione in Libri Contabili e Bilancio ▪ Direzione Amministrativa ▪ Direzione Controllo Gestione & Reporting
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Redazione e deposito bilanci e situazioni contabili annuali e infrannuali ▪ Sistema di controllo incrociati dei flussi informativi registrati nel Sistema Informativo aziendale (SIM Presales e Navision)Bilancio civilistico certificato ▪ Sistema di deleghe ▪ Attività di vigilanza della società di revisione ▪ Attività di vigilanza sulla gestione amministrativa da parte del Collegio Sindacale ▪ Separazione funzioni ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Reati societari (art. 25 ter D.Lgs. 231/2001)	
Modello operativo: Impedito controllo (art. 2625, comma 2, c.c.)	
Processo e Responsabilità	▪ Gestione della Contabilità e Trasposizione in Libri Contabili e Bilancio ▪ Direzione Amministrativa ▪ Direzione Controllo Gestione & Reporting
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Redazione e deposito bilanci e situazioni contabili annuali e infrannuali ▪ Sistema di controllo incrociati dei flussi informativi registrati nel Sistema Informativo aziendale (SIM Presales e Navision) ▪ Bilancio civilistico certificato ▪ Sistema di deleghe ▪ Attività di vigilanza della società di revisione ▪ Attività di vigilanza sulla gestione amministrativa da parte del Collegio Sindacale ▪ Separazione funzioni ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Reati societari (art. 25 ter D.Lgs. 231/2001)	
Modello operativo: Indebita restituzione di conferimenti (art. 2626 c.c.)	
Processo e Responsabilità	▪ Gestione della Contabilità e Trasposizione in Libri Contabili e Bilancio ▪ Direzione Amministrativa ▪ Direzione Controllo Gestione & Reporting
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Redazione e deposito bilanci e situazioni contabili annuali e infrannuali ▪ Sistema di controllo incrociati dei flussi informativi registrati nel Sistema Informativo aziendale (SIM Presales e Navision) ▪ Bilancio civilistico certificato ▪ Attività di vigilanza della società di revisione ▪ Attività di vigilanza sulla gestione amministrativa da parte del Collegio Sindacale ▪ Separazione funzioni ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Reati societari (art. 25 ter D.Lgs. 231/2001)	
Modello operativo: Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)	
Processo e Responsabilità	▪ Gestione della Contabilità e Trasposizione in Libri Contabili e Bilancio ▪ Direzione Amministrativa ▪ Direzione Controllo Gestione & Reporting
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Redazione e deposito bilanci e situazioni contabili annuali e infrannuali ▪ Sistema di controllo incrociati dei flussi informativi registrati nel Sistema Informativo aziendale (SIM Presales e Navision) ▪ Bilancio civilistico certificato ▪ Attività di vigilanza della società di revisione ▪ Attività di vigilanza sulla gestione amministrativa da parte del Collegio Sindacale ▪ Separazione funzioni ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Reati societari (art. 25 ter D.Lgs. 231/2001)	
Modello operativo: Illecite operazioni su azioni o quote sociali o della società controllante (art. 2628 c.c.)	
Processo e Responsabilità	▪ Gestione della Contabilità e Trasposizione in Libri Contabili e Bilancio ▪ Direzione Amministrativa ▪ Direzione Controllo Gestione & Reporting
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Redazione e deposito bilanci e situazioni contabili annuali e infrannuali ▪ Sistema di controllo incrociati dei flussi informativi registrati nel Sistema Informativo aziendale (SIM Presales e Navision) ▪ Bilancio civilistico certificato ▪ Attività di vigilanza della società di revisione ▪ Attività di vigilanza sulla gestione amministrativa da parte del Collegio Sindacale ▪ Separazione funzioni ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Reati societari (art. 25 ter D.Lgs. 231/2001)	
Modello operativo: Operazioni in pregiudizio dei creditori (art. 2629 c.c.)	
Processo e Responsabilità	▪ Gestione della Contabilità e Trasposizione in Libri Contabili e Bilancio ▪ Direzione Amministrativa ▪ Direzione Controllo Gestione & Reporting
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Redazione e deposito bilanci e situazioni contabili annuali e infrannuali ▪ Sistema di controllo incrociati dei flussi informativi registrati nel Sistema Informativo aziendale (SIM Presales e Navision) ▪ Bilancio civilistico certificato ▪ Attività di vigilanza della società di revisione ▪ Attività di vigilanza sulla gestione amministrativa da parte del Collegio Sindacale ▪ Separazione funzioni ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Reati societari (art. 25 ter D.Lgs. 231/2001)	
Modello operativo: Formazione fittizia del capitale (art. 2632 c.c.)	
Processo e Responsabilità	▪ Gestione della Contabilità e Trasposizione in Libri Contabili e Bilancio ▪ Direzione Amministrativa ▪ Direzione Controllo Gestione & Reporting
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Redazione e deposito bilanci e situazioni contabili annuali e infrannuali ▪ Sistema di controllo incrociati dei flussi informativi registrati nel Sistema Informativo aziendale (SIM Presales e Navision) ▪ Bilancio civilistico certificato ▪ Attività di vigilanza della società di revisione ▪ Attività di vigilanza sulla gestione amministrativa da parte del Collegio Sindacale ▪ Separazione funzioni ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Reati societari (art. 25 ter D.Lgs. 231/2001)	
Modello operativo: Corruzione tra privati (art. 2635, comma 3 c.c.)	
Processo e Responsabilità	▪ Pre Vendita e Vendita ▪ Direzione Vendite ▪ Direzione Acquisti ▪ Direzione Acquisti (Responsabile Salute & Sicurezza SSL) ▪ Gestione Risorse Umane (Recruiting) ▪ Direzione HR
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Bilanci annuali e infrannuali ▪ Bilancio civilistico certificato ▪ Controllo note spese - giustificativi ▪ Controllo congruità fatture per servizi: controllo con Direzione Operation per effettuazione reale delle attività di cui alle fatture - controllo congruità con ordine fornitore (ordine cliente - ordine fornitore - fattura) ▪ Controlli tra spese effettuate con carta di credito, causali e relativi giustificativi ▪ Separazione funzioni ▪ Attività di vigilanza sulla gestione amministrativa da parte del Collegio Sindacale ▪ Attività di controllo della Società di revisione ▪ Acquisto servizi da terzi solo in funzione dei uno specifico Ordine Cliente ▪ Fornitori qualificati e registrati in Albo Fornitori ▪ Acquisto diretto da fornitori ▪ Rispetto iter di qualifica e valutazione dei fornitori ▪ Acquisiti legati a specifico ordine/commessa o a una Richiesta di Acquisto (RdA) ▪ Richiesta di Acquisto (RdA) approvata gerarchicamente in relazione al valore economico dell'acquisto e della tipologia ▪ RdA compilata in modo informatico tramite il Sistema Informativo aziendale che in relazione al valore economico e alla tipologia è inoltrata ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Solo le RdA autorizzate possono originare reali esigenze di approvvigionamento ▪ Ordine a fornitore fatto con il Sistema Informativo aziendale attraverso la trasformazione automatica dell'ordine cliente ▪ Accordi quadro con listini e sconti previsti relativamente a Vendor Cliente - Maticmind ▪ Approvazioni a più livelli in base all'entità dell'ordine ▪ Verifiche da parte dell'Ufficio Finanza & Controllo ▪ Definizione poteri di firma del Resp. Acquisiti ▪ Formalizzazione e diffusione iter di selezione ▪ Applicazione iter selezione anche per candidati segnalati direttamente da personale interno ▪ L'autorizzazione alle trasferte è preventivamenterichieste via mail al proprio responsabile e dallo stesso ottenuta tramite il Sistema Informativo aziendale ▪ Previa autorizzazione, le segreterie provvedono alle prenotazioni degli alberghi e all'acquisto dei titoli di viaggio secondo i criteri definiti da Risorse Umane ▪ Le trasferte all'estero sono richieste tramite apposito modulo e autorizzate dalla Direzione ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)

Reati societari (art. 25 ter D.Lgs. 231/2001)	
Modello operativo: Corruzione tra privati (art. 2635, comma 3 c.c.)	
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare ▪
Rischio Residuo	BASSO

Delitti contro la personalità individuale (Art. 25-quinquies D.lgs. 231/2001)	
Modello operativo: Pornografia minorile (art. 600-ter c.p.) da cancellare - Riserva di valutazione con OdV	
Processo e Responsabilità	▪ Utilizzo internet e infrastrutture informatiche ▪ Responsabile ICT
Livello di rischio Netto	MEDIO
Procedure in essere	▪ Firewall che blocca gli accessi a siti che non sono utili all'attività aziendale (es. siti pornografici, musicali, ecc.) ▪ Redazione, aggiornamento e diffusione dei documenti inerenti le politiche e le istruzioni operative per la sicurezza del patrimonio informativo
Livello di rischio Lordo	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti contro la personalità individuale (Art. 25-quinquies D.lgs. 231/2001)	
Modello operativo: Detenzione di materiale pornografico (art. 600-quater c.p.) da cancellare - Riserva di valutazione con OdV	
Processo e Responsabilità	▪ Utilizzo internet e infrastrutture informatiche ▪ Responsabile SI
Livello di rischio Netto	MEDIO
Procedure in essere	▪ Firewall che blocca gli accessi a siti che non sono utili all'attività aziendale (es. siti pornografici, musicali, ecc.) ▪ Redazione, aggiornamento e diffusione dei documenti inerenti le politiche e le istruzioni operative per la sicurezza del patrimonio informativo
Livello di rischio Lordo	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti contro la personalità individuale (Art. 25-quinquies D.lgs. 231/2001)	
Modello operativo: - Pornografia virtuale (art. 600-quater.1 c.p.) da cancellare - Riserva di valutazione con OdV	
Processo e Responsabilità	▪ Utilizzo internet e infrastrutture informatiche ▪ Responsabile SI
Livello di rischio Netto	MEDIO
Procedure in essere	▪ Firewall che blocca gli accessi a siti che non sono utili all'attività aziendale (es. siti pornografici, musicali, ecc.) ▪ Redazione, aggiornamento e diffusione dei documenti inerenti le politiche e le istruzioni operative per la sicurezza del patrimonio informativo
Livello di rischio Lordo	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies D.Lgs. 231/2001)	
Modello operativo: Omicidio colposo (art. 589 c.p.)	
Processo e Responsabilità	▪ Post Vendita ▪ Direzione Operation ▪ Gestione Logistica e Magazzino ▪ Direzione Acquisti
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Rispetto disposizioni Testo Unico 81/2008 “Sistema di Gestione Integrato per la Salute e Sicurezza dei Lavoratori” e norme standard ISO45000 ▪ Aderenza al DVR e alle procedure di sicurezza relative al Sistema di Gestione Integrato ▪ Valutazione rischi interferenziali legati alla realtà lavorativa specifica ▪ Utilizzo DPI in dotazione
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione e diffusione Codici Etico e Disciplinare ▪ Formazione specifica sulla SSL ▪
Rischio Residuo	BASSO

Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies D.Lgs. 231/2001)	
Modello operativo: Lesioni personali colpose (art. 590 c.p.)	
Processo e Responsabilità	▪ Post Vendita ▪ Direzione Operation ▪ Gestione Logistica e Magazzino ▪ Direzione Acquisti ▪
Livello di rischio Lordo	ALTO
Procedure in essere	▪ ▪ Rispetto disposizioni Testo Unico 81/2008 “Sistema di Gestione Integrato per la Salute e Sicurezza dei Lavoratori” e norme standard ISO45000 ▪ Aderenza al DVR e alle procedure di sicurezza relative al Sistema di Gestione Integrato ▪ Valutazione rischi interferenziali legati alla realtà lavorativa specifica ▪ Utilizzo DPI in dotazione
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione e diffusione Codici Etico e Disciplinare ▪ Formazione specifica sulla SSL ▪
Rischio Residuo	BASSO

Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies D.Lgs. 231/2001)	
Modello operativo: Ricettazione (art. 648 c.p.)	
Processo e Responsabilità	▪ Pre Vendita e Acquisti ▪ Direzione Vendite ▪ Direzione Acquisti
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Controllo congruità fatture per servizi: controllo con Funzione interna che ha usufruito dei servizi per effettuazione reale delle attività di cui alle (sigla fattura e mail) - controllo congruità con Ordine Fornitore (Ordine Cliente/RdA - Ordine Fornitore - Fattura) ▪ Pagamenti effettuati solo a fronte di fattura e tramite bonifici ▪ Verifica Revisori dei Conti ▪ Definizione poteri di firma degli amministratori ▪ ▪ Acquisti legati a specifico ordine/commessa o Richiesta di Acquisto (RdA) ▪ RdA compilata in formato elettronico tramite il Sistema Informativo aziendale che in relazione al valore economico e alla tipologia è inoltrata ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Solo le RdA autorizzate possono originare reali esigenze di approvvigionamento ▪ Ordine a fornitore fatto con il Sistema Informativo aziendale attraverso la trasformazione automatica dell'ordine cliente ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciabilità sul Sistema Informativo aziendale di tutti gli ordini (destinati alla vendita) e delle RdA ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies D.Lgs. 231/2001)	
Modello operativo: Riciclaggio (art. 648-bis c.p.)	
Processo e Responsabilità	▪ Pre Vendita e Acquisti e Fatturazione ▪ Direzione Vendite ▪ Direzione Acquisti ▪ Direzione Amministrativa
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Controllo congruità fatture per servizi: controllo con Funzione interna che ha usufruito dei servizi per effettuazione reale delle attività di cui alle (sigla fattura e mail) - controllo congruità con Ordine Fornitore (Ordine Cliente/RdA - Ordine Fornitore - Fattura) ▪ Pagamenti effettuati solo a fronte di fattura e tramite bonifici ▪ Verifica Revisori dei Conti ▪ Definizione poteri di firma degli amministratori ▪ Acquisti legati a specifico ordine/commessa o Richiesta di Acquisto (RdA) ▪ RdA compilata in formato elettronico tramite il Sistema Informativo aziendale che in relazione al valore economico e alla tipologia è inoltrata ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Solo le RdA autorizzate possono originare reali esigenze di approvvigionamento ▪ Ordine a fornitore fatto con il Sistema Informativo aziendale attraverso la trasformazione automatica dell'ordine cliente ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciabilità sul Sistema Informativo aziendale di tutti gli ordini (destinati alla vendita) e delle RdA ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies D.Lgs. 231/2001)	
Modello operativo: Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)	
Processo e Responsabilità	▪ Pre Vendita e Acquisti e Fatturazione ▪ Direzione Vendite ▪ Direzione Acquisti ▪ Direzione Amministrativa
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Controllo congruità fatture per servizi: controllo con Funzione interna che ha usufruito dei servizi per effettuazione reale delle attività di cui alle (sigla fattura e mail) - controllo congruità con Ordine Fornitore (Ordine Cliente/RdA - Ordine Fornitore - Fattura) ▪ Pagamenti effettuati solo a fronte di fattura e tramite bonifici ▪ Verifica Revisori dei Conti ▪ Definizione poteri di firma degli amministratori ▪ Acquisti legati a specifico ordine/commessa o Richiesta di Acquisto (RdA) ▪ RdA compilata in formato elettronico tramite il Sistema Informativo aziendale che in relazione al valore economico e alla tipologia è inoltrata ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Solo le RdA autorizzate possono originare reali esigenze di approvvigionamento ▪ Ordine a fornitore fatto con il Sistema Informativo aziendale attraverso la trasformazione automatica dell'ordine cliente ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciabilità sul Sistema Informativo aziendale di tutti gli ordini (destinati alla vendita) e delle RdA ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codici Etico e Disciplinare
Rischio Residuo	BASSO

Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies D.Lgs. 231/2001)	
Modello operativo: Autoriciclaggio (art. 648-ter.1 c.p.)	
Processo e Responsabilità	▪ Direzione Vendite ▪ Pre Vendita e Acquisti e Fatturazione ▪ Direzione Vendite ▪ Direzione Acquisti ▪ Direzione Amministrativa
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Controllo congruità fatture per servizi: controllo con Funzione interna che ha usufruito dei servizi per effettuazione reale delle attività di cui alle (sigla fattura e mail) - controllo congruità con Ordine Fornitore (Ordine Cliente/RdA - Ordine Fornitore - Fattura) ▪ Pagamenti effettuati solo a fronte di fattura e tramite bonifici ▪ Verifica Revisori dei Conti ▪ Definizione poteri di firma degli amministratori ▪ Acquisti legati a specifico ordine/commessa o Richiesta di Acquisto (RdA) ▪ RdA compilata in formato elettronico tramite il Sistema Informativo aziendale che in relazione al valore economico e alla tipologia è inoltrata ai vari responsabili aziendali coinvolti per l'autorizzazione ▪ Solo le RdA autorizzate possono originare reali esigenze di approvvigionamento ▪ Ordine a fornitore fatto con il Sistema Informativo aziendale attraverso la trasformazione automatica dell'ordine cliente ▪ Ordini emessi sul portale dei carrier previa autorizzazione della Direzione ▪ Tracciabilità sul Sistema Informativo aziendale di tutti gli ordini (destinati alla vendita) e delle RdA ▪ Archiviazione di tutta la documentazione amministrativa a supporto nel Sistema Informativo aziendale (Presales e Navision)
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codice Etico e Disciplinare
Rischio Residuo	BASSO

Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001) da cancellare - Riserva di valutazione con OdV	
Modello operativo: Messa a disposizione del pubblico in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, e senza averne diritto di un'opera o di parte di un'opera dell'ingegno protetta (art. 171, co. 1, lett a-bis e co. 3, L. 633/1941)	
Processo e Responsabilità	▪ Direzione Vendite ▪ Post Vendita ▪ Direzione Operation ▪ Gestione Sistema Informativo ▪ Sistemi informativi
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Vendita dell'attività di implementazione dell'applicativo con obbligo per il cliente di acquisire la relativa licenza ▪ Acquisito diretto da Vendor ▪ Licenze acquistate dal vendor con apparati ▪ Tracciatura seriali dal Vendor ▪ MRA solo su originali tracciati con seriale ▪ Controlli in accettazione ▪ Configurazione standard dei PC dei dipendenti ▪ Dotazioni/tool/SW resi disponibili dai vendor ▪ Gestione informatizzata delle richieste (TTK) formalizzate attraverso il Sistema Informativo aziendale ▪ Impegno sottoscritto dai dipendenti per il rispetto dei criteri generali di tutela del patrimonio informatico ▪ Inventario HW e SW, gestito con il SIM, che consente di gestire le licenze per apparecchiature interne
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Firma Impegno da parte dei tecnici ▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001)	
Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale ovvero concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi di protezione di programmi per elaboratori (art. 171-bis, L. 633/1941)	
Processo e Responsabilità	▪ Pre Vendita, Post Vendita e Acquisti ▪ Direzione Vendita ▪ Direzione Operation ▪ Direzione Acquisti ▪ Direzione Vendite
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Acquisito diretto da Vendor di apparati e licenze ▪ Tracciatura seriali dal Vendor ▪ MRA solo su originali tracciati con seriale ▪ Controlli incrociati tra documentazione amministrativa (Ordini, Richieste di Acquisto e Fatture) con materiale ▪ Software standard a bordo dei dispositivi in dotazione ai dipendenti acquistato con relative licenze Dotazioni/tool/SW resi disponibili dai vendor ▪ Impegno sottoscritto dai dipendenti per il rispetto dei criteri generali di tutela del patrimonio informatico ▪ Inventario HW e SW, gestito con il SIM, che consente di gestire le licenze per apparecchiature interne
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codice Etico e Disciplinare
Rischio Residuo	BASSO

Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001) da cancellare - Riserva di valutazione con OdV	
Reati commessi a fini di lucro, per uso non personale, e caratterizzati da una delle seguenti condotte descritte all'art. 171-ter, comma 1, L. 633/1941	
Processo e Responsabilità	▪ Vendita licenze e apparati ▪ Direzione Vendite ▪ Acquisizione licenze ▪ Acquisiti ▪ Erogazione servizi di Installazione e manutenzione ▪ Direzione Operation ▪ Gestione Sistema Informativo ▪ Sistemi informativi
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Vendita dell'attività di implementazione dell'applicativo con obbligo per il cliente di acquisire la relativa licenza ▪ Acquisito diretto da Vendor ▪ Licenze acquistate dal Vendor con apparati ▪ Tracciatura seriali dal Vendor ▪ MRA solo su originali tracciati con seriale ▪ Controlli in accettazione ▪ Configurazione standard dei PC dei dipendenti ▪ Dotazioni/tool/SW resi disponibili dai vendor ▪ Gestione informatica delle richieste (TTK) formalizzate attraverso il Sistema Informativo aziendale ▪ Impegno sottoscritto dai dipendenti per il rispetto dei criteri generali di tutela del patrimonio informatico ▪ Inventario HW e SW, gestito con il SIM, che consente di gestire le licenze per apparecchiature interne
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Firma Impegno da parte dei tecnici ▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001) da cancellare - Riserva di valutazione con OdV	
Reati caratterizzati da una delle seguenti condotte descritte all'art. 171-ter, comma 2, L. 633/1941	
Processo e Responsabilità	▪ Vendita licenze e apparati ▪ Direzione Vendite ▪ Acquisizione licenze ▪ Acquisiti ▪ Erogazione servizi di Installazione e manutenzione ▪ Direzione Operation ▪ Gestione Sistema Informativo ▪ Sistemi informativi
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Vendita dell'attività di implementazione dell'applicativo con obbligo per il cliente di acquisire la relativa licenza ▪ Acquisito diretto da Vendor ▪ Licenze acquistate dal vendor con apparati ▪ Tracciatura seriali dal Vendor ▪ MRA solo su originali tracciati con seriale ▪ Controlli in accettazione ▪ Configurazione standard dei PC dei dipendenti ▪ Dotazioni/tool/SW resi disponibili dai vendor ▪ Gestione informatizzata delle richieste (TTK) formalizzate attraverso il Sistema Informativo aziendale ▪ Impegno sottoscritto dai dipendenti per il rispetto dei criteri generali di tutela del patrimonio informatico ▪ Inventario HW e SW, gestito con il SIM, che consente di gestire le licenze per apparecchiature interne
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Firma Impegno da parte dei tecnici ▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001) da cancellare - Riserva di valutazione con OdV	
Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno, da parte di produttori o importatori di tali supporti, ovvero falsa dichiarazione circa l'assolvimento degli obblighi sul contrassegno (art. 171-septies, L. 633/1941)	
Processo e Responsabilità	▪ Vendita licenze e apparati ▪ Direzione Vendite ▪ Acquisizione licenze ▪ Acquisiti ▪ Erogazione servizi di Installazione e manutenzione ▪ Direzione Operation ▪ Gestione Sistema Informativo ▪ Sistemi informativi
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Vendita dell'attività di implementazione dell'applicativo con obbligo per il cliente di acquisire la relativa licenza ▪ Acquisito diretto da Vendor ▪ Licenze acquistate dal vendor con apparati ▪ Tracciatura seriali dal Vendor ▪ MRA solo su originali tracciati con seriale ▪ Controlli in accettazione ▪ Configurazione standard dei PC dei dipendenti ▪ Dotazioni/tool/SW resi disponibili dai Vendor ▪ Gestione informatizzata delle richieste (TTK) formalizzate attraverso il Sistema Informativo aziendale ▪ Impegno sottoscritto dai dipendenti per il rispetto dei criteri generali di tutela del patrimonio informatico ▪ Inventario HW e SW, gestito con il SIM, che consente di gestire le licenze per apparecchiature interne
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Firma Impegno da parte dei tecnici ▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs. 231/2001) da cancellare - Riserva di valutazione con OdV	
Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies, L. 633/1941)	
Processo e Responsabilità	▪ Vendita licenze e apparati ▪ Direzione Vendite ▪ Acquisizione licenze ▪ Acquisiti ▪ Erogazione servizi di Installazione e manutenzione ▪ Direzione Operation ▪ Gestione Sistema Informativo ▪ Sistemi informativi
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Vendita dell'attività di implementazione dell'applicativo con obbligo per il cliente di acquisire la relativa licenza ▪ Acquisito diretto da Vendor ▪ Licenze acquistate dal Vendor con apparati ▪ Tracciatura seriali dal Vendor ▪ MRA solo su originali tracciati con seriale ▪ Controlli in accettazione ▪ Configurazione standard dei PC dei dipendenti ▪ Dotazioni/tool/SW resi disponibili dai Vendor ▪ Gestione informatizzata delle richieste (TTK) formalizzate attraverso il Sistema Informativo aziendale ▪ Impegno sottoscritto dai dipendenti per il rispetto dei criteri generali di tutela del patrimonio informatico ▪ Inventario HW e SW, gestito con il SIM, che consente di gestire le licenze per apparecchiature interne
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Firma Impegno da parte dei tecnici ▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione codici etico e disciplinare
Rischio Residuo	BASSO

Delitti in materia ambientale (art. 25- undecies D.Lgs. 231/2001)	
Modello operativo: Attività di gestione di rifiuti non autorizzata (Art. 256 D. Lgs. 152/2006)	
Processo e Responsabilità	▪ Gestione Magazzino e Logistica ▪ Direzione Acquisti
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Smaltimento rifiuti tramite accordi e contratti con società del settore autorizzate
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Creazione Policy per la Gestione dei Rifiuti ▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codice Etico e disciplinare
Rischio Residuo	BASSO

Delitti in materia ambientale (art. 25- undecies D.Lgs. 231/2001)	
Modello operativo: Traffico illecito di rifiuti (Art. 259, comma 1 D. Lgs. 152/2006)	
Processo e Responsabilità	▪ Gestione Magazzino e Logistica ▪ Direzione Acquisti
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Smaltimento rifiuti tramite accordi e contratti con società del settore autorizzate
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Creazione Policy per la Gestione dei Rifiuti ▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codice Etico e disciplinare
Rischio Residuo	BASSO

Delitti in materia ambientale (art. 25- undecies D.Lgs. 231/2001)	
Modello operativo: Attività organizzate per il traffico illecito di rifiuti (Art. 260 D. Lgs. 152/2006)	
Processo e Responsabilità	▪ Gestione Magazzino e Logistica ▪ Direzione Acquisti
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Smaltimento rifiuti tramite accordi e contratti con società del settore autorizzate
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Creazione Policy per la Gestione dei Rifiuti ▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codice Etico e disciplinare
Rischio Residuo	BASSO

Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25- duodecies D.Lgs. 231/2001)	
Modello operativo: Art. 22, comma 12 bis, D.Lgs. 25 luglio 1998, n. 286 ("Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero")	
Processo e Responsabilità	▪ Gestione delle Risorse Umane (Recruiting)Direzione Risorse Umane ▪ Gestione Fornitori ▪ Direzione Acquisti
Livello di rischio Lordo	ALTO
Procedure in essere	▪ Verifiche mirate in fase di Recruiting di personale Maticmind ▪ Richiesta all'interessato e ottenimento della copia permesso di soggiorno in caso di assunzione di cittadini di paesi terzi ▪ Controllo in fase di Qualificazione del Fornitore ▪ Effettuazione controlli circa la regolarità delle risorse inviate da fornitori o da subappaltatori per conto Maticmind (Distacchi) ▪ Richiesta al fornitore o al subappaltatore e ottenimento di copia del contratto in essere e del permesso di soggiorno di cittadini di paesi terzi impiegati nelle attività per conto Maticmind
Livello di rischio Netto	MEDIO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codice Etico e Disciplinare
Rischio Residuo	BASSO

Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25- duodecies D.Lgs. 231/2001)	
Modello operativo: Definizione di reato transnazionale (Art. 3 - L. 146/2006)	
Processo e Responsabilità	▪ Gestione delle Risorse Umane (Recruiting)Direzione Risorse Umane ▪ Gestione Fornitori ▪ Direzione Acquisti
Livello di rischio Lordo	MEDIO
Procedure in essere	▪ Verifiche mirate in fase di Recruiting di personale Maticmind ▪ Richiesta all'interessato e ottenimento della copia permesso di soggiorno in caso di assunzione di cittadini di paesi terzi ▪ Controllo in fase di Qualificazione del Fornitore ▪ Effettuazione controlli circa la regolarità delle risorse inviate da fornitori o da subappaltatori per conto Maticmind (Distacchi) ▪ Richiesta al fornitore o al subappaltatore e ottenimento di copia del contratto in essere e del permesso di soggiorno di cittadini di paesi terzi impiegati nelle attività per conto Maticmind
Livello di rischio Netto	BASSO
Procedure aggiuntive	▪ Formazione specifica sui reati che insistono sull'area ▪ Formazione e diffusione Codice Etico e Disciplinare ▪
Rischio Residuo	BASSO

13 CROSS MAP: REATI-DOCUMENTAZIONE

Nell'Allegato 1, parte integrante del presente documento, si riporta la correlazione tra reati presupposto ex D.Lgs. 231/2001 e la documentazione a supporto (protocolli interni).

14 IL CODICE ETICO

14.1 RESPONSABILITA' SOCIALE E CODICE ETICO

Maticmind ha preso visione della norma SA8000 (la norma che definisce l'impegno per la responsabilità sociale verso i propri lavoratori e la soddisfazione dei Clienti) e ad essa si ispira nella quotidiana operatività. È conforme a tutti i seguenti paragrafi del capitolo IV della SA8000:2008 e in particolare dichiara di:

- non utilizzare né dare sostegno al lavoro infantile
- non ricorrere a lavoro obbligato di nessun tipo, né richiedere o trattenere depositi o documenti di identità al momento dell'inizio del rapporto di lavoro
- rispettare le norme e le leggi nazionali sulla Salute e Sicurezza dei Lavoratori
- rispettare il diritto di tutto il personale di aderire ai sindacati di propria scelta e il diritto alla contrattazione collettiva, nel rispetto delle normative di legge
- non applicare principi discriminatori di nessun tipo e in nessuna occasione di lavoro (assunzione, remunerazione, formazione, pensionamento, licenziamento), né consentire comportamenti coercitivi, minacciosi, offensivi o volti allo sfruttamento, così come indicato ai § 5.1, 5.2, 5.3 e 5.4 della norma
- non applicare punizioni corporali, ma trattare tutto il personale con dignità e rispetto
- conformarsi all'orario di lavoro stabilito dagli accordi sindacali e non superare in alcun modo le 60 ore settimanali
- rispettare le normative nazionali e la contrattazione collettiva sul lavoro, con particolare riferimento agli standard legali e minimi di settore della retribuzione
- avere ragionevole certezza che i propri subfornitori/subappaltatori soddisfino i requisiti dei precedenti punti.

14.2 ELABORAZIONE ED APPROVAZIONE DEL CODICE ETICO

Maticmind cura con particolare attenzione la valorizzazione e la salvaguardia dei profili etici della propria attività d'impresa, avendo individuato quali valori centrali della propria cultura e dei propri comportamenti i concetti di "legalità" e "integrità".

In questo contesto, Maticmind si è rivelata particolarmente attiva nel garantire una adeguata formazione del personale dipendente, incentrata sulla condivisione della propria cultura di impegno, correttezza e rispetto delle regole.

Nell'ambito di tale attività di formazione, si è provveduto a distribuire a tutti i dipendenti il Codice Etico. In particolare, in ottemperanza al disposto normativo, Maticmind ha predisposto e adotta un documento denominato appunto "*Codice Etico*", costituente parte integrante del *Modello Organizzativo*, con lo scopo di individuare e definire in modo chiaro ed esaustivo l'insieme dei valori, dei principi fondamentali e delle norme comportamentali, che costituiscono il presupposto irrinunciabile per il corretto svolgimento delle attività aziendali.

Ai fini del Decreto, il *Codice Etico* costituisce l'unico riferimento per fornire l'indirizzo etico di tutte le attività della Società.

14.3 DESTINATARI E STRUTTURA DEL CODICE ETICO

Il *Codice Etico* di Maticmind indica i principi generali e le regole comportamentali cui la Società riconosce valore etico positivo e a cui devono conformarsi tutti i Destinatari. Tali sono:

- i rappresentanti degli Organi Sociali (amministratori e sindaci) e i Manager
- tutti i Dipendenti Maticmind
- i Fornitori di beni e servizi, gli Appaltatori, i Consulenti, i Collaboratori e i soggetti incaricati della Revisione della Società.

I Destinatari sono tenuti ad osservare e, per quanto di propria competenza, a fare osservare i principi contenuti nel *Modello Organizzativo* e nel *Codice Etico* che ne è parte, vincolanti per tutti loro e applicabili anche alle attività svolte all'estero.

Il complesso delle regole contenute nel *Codice Etico*, peraltro, uniformando i comportamenti aziendali a standard etici particolarmente elevati e improntati alla massima correttezza e trasparenza, garantisce la possibilità di salvaguardare gli interessi degli stakeholders, nonché di preservare l'immagine e la reputazione della Società, assicurando nel contempo un approccio etico al mercato, con riguardo sia alle attività svolte nell'ambito del territorio italiano sia a quelle relative a rapporti internazionali.
Il corpus del *Codice Etico* è così suddiviso:

- una parte introduttiva, nel cui ambito sono anche indicati i Destinatari
- i principi etici di riferimento, ovvero i valori cui Maticmind dà rilievo nell'ambito della propria attività di impresa e che devono essere rispettati da tutti i Destinatari
- le norme e i principi di comportamento dettati con riguardo alle differenti categoria di Destinatari

Di seguito si riporta una sintesi dei principi etici e delle norme di comportamento che sostanziano il *Codice Etico*, fermo restando che per la sua completa conoscenza si rimanda al "*Codice Etico*" nella sua interezza, che costituisce parte integrante del presente *Modello Organizzativo*.

14.3.1 I Principi Etici Generali

Nella prima sezione del *Codice Etico* sono individuati i principi etici generali che regolano l'attività di Maticmind. Tali principi rappresentano i valori fondamentali cui i soggetti tenuti al rispetto del *Codice Etico* devono attenersi nel perseguimento della mission aziendale e, in genere, nella conduzione delle attività sociali.

In particolare, i principi etici fondamentali adottati da Maticmind riguardano i valori e le aree di attività di seguito elencate:

- responsabilità e rispetto delle leggi
- correttezza
- valore del capitale umano
- tutela della privacy
- informazioni confidenziali e proprietarie

- trasparenza
- riservatezza
- rispetto della dignità della persona
- sostenibilità socio-ambientale
- ripudio di ogni forma di terrorismo
- ripudio di ogni forma di criminalità organizzata.

14.3.2 Principi e Norme di Comportamento

Maticmind ha riservato un'apposita sezione del *Codice Etico* alle norme e ai principi di comportamento che devono essere rispettati nell'ambito dell'attività d'impresa indicando, per ciascuna categoria dei soggetti Destinatari, le norme e i principi di comportamento da seguire.

1. Norme comportamentali nell'ambito della corporate governance

   I componenti degli **organi sociali**, in ragione del loro fondamentale ruolo, anche qualora non siano dipendenti della Società, sono tenuti a rispettare le previsioni del *Modello Organizzativo* e del *Codice Etico* che ne è parte.

   In particolare, nello svolgimento della loro attività, essi devono tenere un comportamento ispirato ad autonomia, legalità e correttezza nei rapporti con qualsivoglia interlocutore, sia pubblico sia privato. Ugualmente, devono tenere un comportamento responsabile, leale e trasparente nei confronti della Società e astenersi dal compiere atti in presenza di un conflitto di interesse.

   Nei confronti degli **azionisti**, Maticmind promuove la trasparenza e l'informazione periodica, nel rispetto delle leggi e delle norme vigenti. Le informazioni che vengono trasmesse agli azionisti saranno vere, complete e rifletteranno la situazione della Società.

   Maticmind promuove la massima riservatezza delle informazioni inerenti operazioni straordinarie. I Destinatari coinvolti dovranno mantenere riservate tali informazioni e non abusarne.

   La Società tutela e accresce il valore dell'impresa con l'obiettivo di premiare il rischio assunto dagli azionisti nell'investimento dei propri capitali, pertanto si impegna a proteggere, conservare e aumentare i beni, i diritti e i legittimi interessi degli azionisti rispettando gli accordi stipulati.

   Nei confronti del **mercato**, Maticmind riconosce il valore della concorrenza ispirato ai principi di correttezza, leale competizione e trasparenza nei confronti dei competitor presenti sul mercato:
   - proibendo condotte che, integrando intese restrittive della concorrenza e/o abusi di posizione dominante, consentano, singolarmente o congiuntamente ad altre organizzazioni, di pregiudicare la regolare competizione economica (antitrust)
   - impegnandosi a competere sul mercato in modo leale, sollecitando la libera concorrenza nel pieno rispetto della normativa vigente ed evitando qualunque condotta che costituisca abuso, restrizione o violazione della stessa (conflitto di interessi)
   - non perseguendo vantaggi competitivi attraverso pratiche commerciali illegali o immorali (pratiche commerciali etiche)

- garantendo la massima trasparenza nelle transazioni commerciali e predisponendo gli strumenti più opportuni al fine di contrastare i fenomeni del riciclaggio e della ricettazione (tutela della trasparenza nelle transazioni commerciali e anti-riciclaggio)
- rispettando gli organi di informazione e garantendo informazioni e comunicazioni accurate, veritiere, complete, trasparenti e tra loro omogenee, fornite esclusivamente dalle funzioni aziendali a ciò preposte.

Maticmind promuove la massima trasparenza, affidabilità e integrità delle informazioni inerenti alla contabilità aziendale. Ogni operazione e transazione deve essere correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua.

2. Norme comportamentali nelle relazioni con il personale

Il Personale deve informare la propria condotta, sia nei rapporti interni che nei confronti degli interlocutori esterni alla Società, alla normativa vigente, ai principi espressi nel *Codice Etico* e alle norme di comportamento appositamente indicate, nel rispetto del *Modello Organizzativo* e delle procedure aziendali vigenti.

In via generale, il personale Maticmind deve evitare di porre in essere, di dar causa o di collaborare alla realizzazione di comportamenti idonei, anche in via potenziale, a integrare alcuna delle fattispecie di reato richiamate nel Decreto, nonché deve collaborare con l'Organismo di Vigilanza nel corso delle attività di verifica e vigilanza da questo espletate, fornendo le informazioni, i dati e le notizie da esso richieste.
In particolare, nelle attività di **selezione e reclutamento**, i Destinatari promuovono il rispetto dei principi di eguaglianza e di pari opportunità nelle attività di selezione e reclutamento del personale, rifiutando qualunque forma di favoritismo, nepotismo o clientelismo e ripudiando ogni principio di discriminazione.

Inoltre, i rapporti di lavoro sono **formalizzati** con regolare contratto, rifiutando qualunque forma di lavoro irregolare.

Maticmind persegue con il massimo impegno l'obiettivo di garantire la **salute e la sicurezza dei luoghi di lavoro**. La Società favorisce condizioni di lavoro che tutelano l'integrità psico-fisica delle persone, mettendo a disposizione luoghi di lavoro conformi alle vigenti normative in materia di salute e sicurezza.

Promuove, inoltre, la **crescita professionale** dei collaboratori, mediante opportuni strumenti e piani formativi.

La **protezione e conservazione dei beni aziendali** costituisce un valore fondamentale per la salvaguardia degli interessi societari ed è cura del personale, nell'espletamento delle proprie attività aziendali non solo proteggere tali beni, ma impedirne l'uso fraudolento o improprio.

Il Personale, nello svolgimento delle proprie attività professionali, deve utilizzare gli strumenti e i servizi informatici o telematici nel pieno rispetto delle vigenti normative in materia (particolarmente in tema di illeciti informatici, sicurezza informatica, privacy e diritto d'autore) e delle procedure interne.
A riguardo, è fatto espresso divieto di utilizzare le informazioni riservate del cliente per perpetrare crimini informatici.

Ciascun dipendente deve astenersi dal prestare la propria attività sotto l'effetto di sostanze alcoliche o stupefacenti, o che sortiscano analogo effetto e di consumare o cedere a qualsiasi titolo tali sostanze nel corso della prestazione lavorativa e deve rispettare il divieto di fumare di cui all'art 51 della legge 16/01/2003 n. 3.

Maticmind esige che nelle relazioni di lavoro interne ed esterne non si verifichino molestie di alcun genere.

3. Norme comportamentali nei confronti di terzi

Come sopra rilevato, il *Modello Organizzativo* e il *Codice Etico* si applicano anche ai terzi, ovvero ai soggetti esterni alla Società che operano, direttamente o indirettamente, per il raggiungimento degli obiettivi di quest'ultima.

Tali soggetti, nei limiti delle rispettive competenze e responsabilità, sono obbligati al rispetto delle disposizioni del *Modello Organizzativo* e del *Codice Etico* che ne è parte, inclusi i principi etici generali.
In particolare, nei confronti dei clienti, Maticmind ha come obiettivo la soddisfazione delle necessità degli stessi in maniera affidabile e competitiva attraverso relazioni improntate alla massima imparzialità.

A tale scopo, tutti i soggetti interessati da tale processo devono promuovere con i clienti relazioni commerciali durature, basate sulla capacità di fornire un servizio con continuità e di apportare valore aggiunto, sviluppando a tal fine soluzioni che vadano oltre le aspettative dei clienti stessi e che non implichino rischi per la loro salute o sicurezza, rispettando gli accordi concordati.

Maticmind garantisce la riservatezza dei dati dei propri clienti, impegnandosi a non rivelarli a terzi, salvo previo consenso del cliente o per obblighi di tipo legale o per compiere risoluzioni giudiziali o amministrative.

I processi di selezione e scelta dei fornitori sono improntati a principi di legalità, correttezza e trasparenza.

La scelta del **fornitore** si basa su criteri oggettivi e imparziali in termini di qualità, affidabilità, costo, servizi aggiuntivi rispetto ai servizi/prodotti offerti.

Inoltre, Maticmind si impegna a esigere dai propri fornitori il rispetto della normativa in materia di lavoro, ivi incluso ciò che attiene al lavoro minorile e delle donne, alla salute e sicurezza dei lavoratori, ai diritti sindacali o comunque di associazione e rappresentanza.

Nei rapporti con la **Pubblica Amministrazione e le Pubbliche Istituzioni**, i Destinatari promuovono rapporti leciti e corretti nell'ambito della massima trasparenza e rifiutano qualunque forma di promessa od offerta di pagamenti o beni per promuovere o favorire qualsiasi interesse o vantaggio.

Maticmind ripudia esplicitamente qualsiasi pratica corruttiva nella gestione dei rapporti con le istituzioni pubbliche e, in generale, con la Pubblica Amministrazione Italiana e con gli organi della Comunità Europea.

Nel caso specifico dell'effettuazione di una gara, si deve operare nel rispetto delle leggi vigenti e della corretta pratica commerciale.

Gli omaggi e gli atti di cortesia verso Pubblici Ufficiali, Incaricati di Pubblico Servizio o comunque pubblici dipendenti, sono consentititi solo quando, essendo di modico valore, non compromettano in alcun modo l'integrità e l'indipendenza delle parti e non possano essere interpretati come strumento per ottenere vantaggi in modo improprio.

Maticmind non eroga contributi di alcun genere, direttamente o indirettamente, a partiti politici, movimenti, comitati e organizzazioni politiche e sindacali, né a loro rappresentanti o candidati, sia in Italia che all'Estero, ad esclusione dei contributi consentiti sulla base di specifiche normative.

14.4 Gli Obblighi di Comunicazione all'Organismo di Vigilanza

I Destinatari del *Codice Etico* devono adempiere a precisi obblighi di informazione nei confronti dell'Organismo di Vigilanza, con particolare riferimento alle possibili violazioni di norme di legge o regolamenti, del *Modello Organizzativo*, del *Codice Etico* e delle procedure interne.

Le comunicazioni all'Organismo di Vigilanza sono effettuate a mezzo e-mail.

In ogni caso, l'Organismo di Vigilanza si adopera affinché la persona che effettua la comunicazione, qualora identificata o identificabile, non sia oggetto di ritorsioni, discriminazioni o, comunque, penalizzazioni, assicurandone, quindi, la riservatezza (salvo la ricorrenza di eventuali obblighi di legge che impongano diversamente) [si rimanda, in proposito, al documento "*MM_PAQ231_04_WHISTLEBLOWING POLICY*", parte integrante del presente Modello].

14.5 Le Modalità di Attuazione e Controllo sul Rispetto del Codice Etico

Il controllo circa l'attuazione e il rispetto del *Modello Organizzativo* e del *Codice Etico* è affidato all'Organismo di Vigilanza, il quale è tenuto, tra l'altro, a:

- vigilare sul rispetto del *Modello Organizzativo* e del *Codice Etico*, nell'ottica di ridurre il pericolo di commissione dei reati previsti dal Decreto
- formulare le proprie osservazioni in merito sia alle problematiche di natura etica che dovessero insorgere nell'ambito delle decisioni aziendali, sia alle presunte violazioni del *Modello Organizzativo* o del *Codice Etico* di cui venga a conoscenza
- fornire ai soggetti interessati tutti i chiarimenti e le delucidazioni richieste, ivi incluse quelle relative alla legittimità di un comportamento o condotta concreti, ovvero alla corretta interpretazione delle previsioni del *Modello Organizzativo* o del *Codice Etico*
- seguire e coordinare l'aggiornamento del *Modello Organizzativo* e del *Codice Etico*, anche attraverso proprie proposte di adeguamento e/o aggiornamento
- promuovere e monitorare l'implementazione, da parte della Società, delle attività di comunicazione e formazione sul *Modello Organizzativo* e, in particolare, sul *Codice Etico*
- segnalare agli organi aziendali competenti le eventuali violazioni del *Modello Organizzativo* o del *Codice Etico*, proponendo la sanzione da irrogare nei confronti del soggetto individuato quale responsabile e verificando l'effettiva applicazione delle sanzioni eventualmente irrogate.

15 IL SISTEMA DISCIPLINARE

Ai sensi degli artt. 6 e 7 del Decreto, il *Modello Organizzativo* può ritenersi efficacemente attuato, ai fini dell'esclusione di responsabilità della Società, se prevede un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure ivi indicate.

15.1 Funzione e principi del sistema disciplinare

Ai fini dell'esimente della responsabilità della Società, gli artt. 6 e 7 del D.Lgs. 231/01 pongono fra i requisiti essenziali del *Modello Organizzativo* la previsione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle regole di condotta e delle procedure del *Modello Organizzativo* prescritte per la prevenzione dei reati.

In particolare, il sistema di sanzioni commisurate alla condotta e applicabili in caso di violazione delle regole, oltre all'effetto deterrente per la commissione di illeciti, permette un'efficace azione di controllo dell'Organismo di Vigilanza e garantisce l'effettività del *Modello Organizzativo*, tanto più che l'applicazione delle Sanzioni Disciplinari prescinde dall'esito di qualsiasi procedimento, anche penale, avviato innanzi l'autorità giudiziaria, in quanto le norme previste dal *Modello Organizzativo* sono assunte dalla Società in piena autonomia, indipendentemente dall'illecito penale, amministrativo o civile, che possa scaturire dalla condotta sanzionata.

Maticmind ha quindi definito – in un apposito *Codice Disciplinare* – e adottato un sistema disciplinare precipuamente volto a sanzionare la violazione dei principi, delle norme e delle misure previste nel *Modello Organizzativo* e nei documenti che di esso fanno parte, nel rispetto delle norme previste dalla contrattazione collettiva nazionale, nonché delle norme di legge o di regolamento vigenti.

Sulla scorta di tale Sistema Disciplinare sono passibili di sanzione sia le violazioni del *Modello Organizzativo* e dei relativi documenti commesse dai soggetti posti in posizione apicale, sia le violazioni perpetrate dai soggetti in posizione subordinata, in quanto sottoposti all'altrui direzione o vigilanza o operanti in nome e/o per conto di Maticmind. I sanzionati lo sono in quanto titolari di funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia funzionale, ovvero titolari del potere anche solo di fatto, di gestione o di controllo della Società stessa.

L'instaurazione di un procedimento disciplinare, così come l'applicazione delle relative sanzioni, prescindono dall'eventuale instaurazione e/o dall'esito di eventuali procedimenti penali aventi ad oggetto le medesime condotte rilevanti ai fini del Sistema Disciplinare.

15.2 La Struttura del Sistema Disciplinare

Il Sistema Disciplinare di Maticmind si articola in quattro sezioni inerenti ognuna una categoria di soggetti passibili delle sanzioni ivi previste, rappresentati da:

- Lavoratori Subordinati
- Dirigenti
- Vertici Aziendali
- Collaboratori e consulenti

Per ogni sezione sono definite:

- le **violazioni** del *Modello Organizzativo* con una elencazione esemplificativa e non tassativa delle condotte, commissive o omissive (anche colpose), idonee a ledere l'efficacia dello stesso quale strumento di prevenzione del rischio di commissione dei reati rilevanti ai fini del Decreto
- le **sanzioni** previste dal CCNL vigente, applicabili in ragione della gravità delle inosservanze.

15.3 Tipologia e Criteri di Applicazione delle Sanzioni

La condotta tenuta dal lavoratore dipendente in violazione delle norme di comportamento previste dal *Modello Organizzativo* e dai documenti che ne costituiscono parte integrante, costituisce un illecito disciplinare.

Le sanzioni irrogabili nei confronti di un lavoratore dipendente sono dettate nel rispetto dell'art. 7 Legge 300/1970 (Statuto dei Lavoratori) e sono riconducibili alle sanzioni previste dall'apparato sanzionatorio di cui al vigente CCNL (TITOLO VII "Rapporti in azienda" – art. 8 Provvedimenti disciplinari) e precisamente:

a) richiamo verbale
b) ammonizione scritta
c) multa non superiore a tre ore di retribuzione oraria calcolata sul minimo tabellare
d) sospensione della retribuzione e dal servizio fino a un massimo di 3 giorni
e) licenziamenti senza preavviso.

Le sanzioni e il risarcimento degli eventuali danni sono commisurate alla condotta e alle conseguenze disciplinari, tenendo in particolare considerazione:

- il livello di responsabilità gerarchica e autonomia del Dipendente
- l'esistenza di precedenti disciplinari a carico del Dipendente
- l'elemento soggettivo del comportamento (dolo, colpa lieve o grave)
- la rilevanza degli obblighi violati
- l'entità del danno derivante alla Società
- l'entità del danno alla Società per l'eventuale applicazione delle sanzioni previste dal Decreto
- l'eventuale condivisione di responsabilità con altri dipendenti che abbiano concorso nel determinare la violazione
- altre circostanze in cui è maturata la violazione del *Modello Organizzativo*.

Di seguito si riporta una sintesi del sistema sanzionatorio previsto per le diverse categorie di lavoratori, fermo restando che per la completa disanima del sistema in oggetto si rimanda all'apposito *Codice Disciplinare*.

15.3.1 Misure nei confronti dei Lavoratori Subordinati

Le sanzioni previste di seguito si applicano nei confronti di quadri e impiegati alle dipendenze della Società che pongano in essere illeciti disciplinari derivanti da:

- mancato rispetto dei principi di comportamento e dei protocolli indicati nel *Modello Organizzativo*
- mancata o non veritiera evidenza dell'attività svolta relativamente alle modalità di documentazione, di conservazione e di controllo degli atti relativi alle procedure correlate, in modo da impedire la trasparenza e verificabilità della stessa
- violazione e/o elusione del sistema di controllo, posta in essere mediante la sottrazione, la distribuzione o l'alterazione della documentazione prevista dalle procedure ovvero con l'impedimento ai soggetti preposti e all'Organismo di Vigilanza del controllo o dell'accesso alle informazioni richieste e alla documentazione
- inosservanza delle disposizioni relative ai poteri di firma e al sistema delle deleghe
- omessa vigilanza da parte dei superiori gerarchici sui propri sottoposti circa la corretta e l'effettiva applicazione dei principi di comportamento e dei protocolli indicati nel *Modello Organizzativo*.

Il mancato rispetto delle misure e delle procedure indicate nel *Modello Organizzativo* e nel *Codice Etico*, a seconda della gravità dell'infrazione, è sanzionato con i seguenti provvedimenti disciplinari:

a) richiamo verbale: comminato nei casi di lieve violazione colposa dei Principi Etici, delle Norme comportamentali e/o delle Procedure previste dal *Modello Organizzativo* o di errori procedurali dovuti a negligenza
b) ammonizione scritta: comminata nei casi di recidiva nelle violazioni che comportano un richiamo verbale
c) multa: comminata oltre che nei casi di recidiva nella commissione di infrazioni da cui possa derivare l'applicazione dell'ammonizione scritta, nei casi in cui, per il livello di responsabilità gerarchico o tecnico, o in presenza di circostanze aggravanti, il comportamento colposo e/o negligente possa compromettere, sia pure a livello potenziale, l'efficacia del *Modello Organizzativo*
d) sospensione dalla retribuzione e dal servizio, per un massimo di 3 giorni: comminata nei casi di gravi violazioni delle Norme comportamentali e/o delle Procedure, tali da esporre Maticmind a responsabilità nei confronti dei terzi, nonché nei casi di recidiva nella commissione di infrazioni da cui possa derivare l'applicazione della multa
e) licenziamento senza preavviso: comminata per mancanze così gravi da far venir meno il rapporto fiduciario con la Società e non consentire, pertanto, la prosecuzione neppure provvisoria del rapporto di lavoro, quali a titolo esemplificativo e non tassativo:
    - violazione delle Norme comportamentali e delle procedure aventi rilevanza esterna e/o elusione fraudolenta delle stesse, realizzata con un comportamento diretto alla commissione di un reato ricompreso fra quelli previsti nel D.Lgs. 231/2001
    - violazione e/o elusione del sistema di controllo, poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione prevista dalle procedure ovvero con l'impedimento ai soggetti preposti e all'Organismo di Vigilanza del controllo o dell'accesso alle informazioni richieste e alla documentazione.

Le predette sanzioni si applicano anche nel caso di violazione della c.d. normativa sul *whistleblowing,* di cui al D.Lgs. n. 24 del 10 marzo 2023 e della relativa procedura adottata da Maticmind, alla quale si rinvia integralmente.

15.3.2 Misure nei confronti dei Dirigenti

Le sanzioni previste di seguito si applicano nei confronti dei dirigenti che pongano in essere illeciti disciplinari derivanti da:

- mancato rispetto delle Norme comportamentali e delle procedure indicate nel *Modello Organizzativo*
- mancata o non veritiera evidenza dell'attività svolta relativamente alle modalità di documentazione, di conservazione e di controllo degli atti relativi alle procedure in modo da impedire la trasparenza e verificabilità della stessa
- violazione e/o elusione del sistema di controllo poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione prevista dalle procedure ovvero con l'impedimento ai soggetti preposti e all'Organismo di Vigilanza del controllo o dell'accesso alle informazioni richieste e alla documentazione
- inosservanza delle disposizioni relative ai poteri di firma e al sistema delle deleghe, ad eccezione dei casi di estrema necessità e di urgenza, di cui deve essere data tempestiva informazione al superiore gerarchico
- omessa supervisione, controllo e vigilanza da parte dei superiori gerarchici sui propri sottoposti circa la corretta e l'effettiva applicazione dei Principi Etici e delle procedure indicati nel *Modello Organizzativo*
- inosservanza dell'obbligo di informativa all'Organismo di Vigilanza e/o al diretto superiore gerarchico circa eventuali violazioni del *Modello Organizzativo* poste in essere da altri dipendenti, di cui si abbia prova diretta e certa
- se di competenza, mancata formazione e/o mancato aggiornamento e/o omessa comunicazione al personale sottoposto alla propria direzione, operante nell'ambito dei processi regolati dalle procedure.

La commissione degli illeciti disciplinari di cui sopra da parte dei dirigenti è sanzionato, tenuto conto della particolare natura fiduciaria del rapporto di lavoro, con il seguente provvedimento disciplinare:

a) licenziamento senza preavviso: comminato nei casi da cui derivi una lesione del rapporto di fiducia tale da non consentire la prosecuzione, anche provvisoria, del rapporto di lavoro.

Le predette sanzioni si applicano anche nel caso di violazione della c.d. normativa sul *whistleblowing,* di cui al D.Lgs. n. 24 del 10 marzo 2023 e della relativa procedura adottata da Maticmind, alla quale si rinvia integralmente.

15.3.3 Misure nei Confronti dei Vertici Aziendali

Le sanzioni previste di seguito si applicano nei confronti di Presidente, Amministratore Delegato, altri membri del Consiglio di Amministrazione, Direttore del Personale, Direttore delle Operation / Direttore Tecnico, Direttori Commerciali, Chief Financial Officer, Direttore Compliance e Direttori a capo delle Business Units, che pongano in essere illeciti disciplinari derivanti da:

- mancato rispetto delle Norme comportamentali e delle procedure contenuti nel *Modello Organizzativo*
- violazione e/o elusione del sistema di controllo poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione prevista dalle procedure ovvero con l'impedimento ai soggetti preposti e all'Organismo di Vigilanza del controllo o dell'accesso alle informazioni richieste e alla documentazione
- violazione delle disposizioni relative ai poteri di firma e, in generale, al sistema delle deleghe, ad eccezione dei casi di necessità e di urgenza, di cui deve essere data tempestiva informazione al Consiglio di Amministrazione

- violazione dell'obbligo di informativa all'Organismo di Vigilanza e/o all'eventuale soggetto sovraordinato circa comportamenti diretti alla commissione di un reato ricompreso fra quelli previsti dal D.Lgs. 231/2001.

A seconda della gravità dell'infrazione e su conforme decisione del Consiglio di Amministrazione, sentito il Collegio Sindacale, potranno essere applicate misure di tutela, nell'ambito di quelle previste dalla vigente normativa in materia di rapporti societari.

Qualora il soggetto sia impiegato/quadro/dirigente della Società, nel rispetto della procedura prevista dall'art. 7 dello Statuto dei lavoratori e del rispettivo CCNL, il Consiglio di Amministrazione adotta le specifiche misure sanzionatorie già sopra indicate per quadri e impiegati e per i dirigenti.

Nei casi più gravi, il Consiglio di Amministrazione, sentito il Collegio Sindacale, può proporre all'Assemblea di procedere anche alla revoca dell'incarico conferito, secondo quanto previsto dalle norme in materia di rapporti societari.

Le predette sanzioni si applicano anche nel caso di violazione della c.d. normativa sul *whistleblowing,* di cui al D.Lgs. n. 24 del 10 marzo 2023 e della relativa procedura adottata da Maticmind, alla quale si rinvia integralmente.

15.3.4 Misure nei Confronti di Collaboratori e Consulenti

Le sanzioni previste di seguito si applicano nei confronti di collaboratori e consulenti esterni che pongano in essere comportamenti non conformi alle prescrizioni e agli obblighi contenuti nei contratti di collaborazione o nelle lettere di incarico.

illeciti disciplinari derivanti da:

- elusione fraudolenta delle Norme comportamentali e delle procedure attinenti all'oggetto dell'incarico, aventi rilevanza esterna ovvero violazione delle stesse realizzata attraverso un comportamento diretto alla commissione di un reato ricompreso fra quelli previsti nel D.Lgs. 231/2001
- violazione e/o elusione del sistema di controllo, poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione prevista dalle procedure attinenti all'incarico ovvero con l'impedimento ai soggetti preposti e all'Organismo di Vigilanza del controllo o dell'accesso alle informazioni richieste e alla documentazione
- mancata, incompleta o non veritiera documentazione dell'attività svolta, tale da impedire la trasparenza e verificabilità della stessa.

Nei confronti di coloro che, in qualità di collaboratori o consulenti di Maticmind e soggetti al coordinamento o vigilanza da parte della stessa, abbiano posto in essere comportamenti non conformi alle prescrizioni e agli obblighi contenuti nei contratti di collaborazione o nelle lettere di incarico del *Modello Organizzativo* sopra indicate, in mancanza di una specifica clausola contrattuale può essere comunque invocata la risoluzione di diritto del rapporto contrattuale ai sensi dell'art. 1456 C.C..

16 L'ORGANISMO DI VIGILANZA

Di seguito si sintetizzano i principali aspetti inerenti all'Organismo di Vigilanza, rimandando per quanto riguarda gli ulteriori aspetti al documento "*Regolamento dell'Organismo di Vigilanza*", parte integrante del presente *Modello Organizzativo*.

16.1 Criteri di Scelta dei Componenti l'Organismo di Vigilanza

Nel prendere atto che la legge non fornisce indicazioni dettagliate circa la composizione dell'Organismo di Vigilanza, Maticmind ha optato per l'organismo collegiale, costituito da tre membri, al fine di garantire l'effettività dei controlli in relazione alla dimensione e alla complessità organizzativa.

In particolare, i componenti dell'Organismo di Vigilanza sono di volta in volta individuati nel rispetto delle seguenti indicazioni:

1. un professionista esterno alla Società, con comprovata competenza ed esperienza in relazione a tematiche aziendali e alle attività ispettive e di analisi dei sistemi di controllo interni
2. un professionista esterno alla Società, con comprovata competenza ed esperienza di tipo giuridico, inclusi gli aspetti di diritto penale
3. un professionista esterno alla Società esperto in materia fiscale, tributaria e giuridica delle gestioni patrimoniali tale da fornire adeguato supporto dell'attività ispettiva e di analisi del sistema di controllo.

Tali soggetti hanno provata esperienza e devono possedere sia i requisiti di autonomia, indipendenza, onorabilità, professionalità, continuità d'azione richiesti, sia specifiche capacità in tema di attività ispettive e consulenziali.

La definizione del Regolamento dell'Organismo di Vigilanza è lasciata ai componenti incaricati, i quali avranno cura di farlo verificare dal Consiglio di Amministrazione, al fine di garantire omogeneità di condotta e rispetto delle direttive aziendali.

16.2 Caratteristiche dell'Organismo di Vigilanza

L'Organismo di Vigilanza di Maticmind è conforme ai requisiti prescritti dal D.Lgs. 231/01, che richiede autonomi poteri di iniziativa e di controllo e, dunque, è dotato di:

a) **Autonomia**

Nell'ambito dello svolgimento della propria funzione, l'Organismo di Vigilanza:

- non è soggetto al potere gerarchico e disciplinare di alcun organo o funzione societaria, ma riporta direttamente al Consiglio di Amministrazione, in quanto massimo vertice operativo della Società
- non svolge attività di gestione o incarichi di natura operativa che, rendendolo partecipe di decisioni e attività operative, ne metterebbero a repentaglio l'obiettività di giudizio
- ha facoltà di auto-determinazione delle proprie regole comportamentali o procedurali e di autonomia nel controllo, grazie al libero accesso a informazioni e documentazione
- è dotato di adeguate risorse finanziarie e strutturali.

b) **Indipendenza**

L'Organismo di Vigilanza è un organo privo di legami di sudditanza nei confronti della Società e del suo management, collocato al vertice aziendale e le cui scelte non sono sindacabili.

c) **Professionalità**

I membri dell'Organismo di Vigilanza hanno competenze tecnico professionali adeguate alle funzioni che sono chiamati a svolgere in termini di:

- capacità e affidabilità
- professionalità specifiche
- competenze multidisciplinari (natura societaria, penale, organizzativa, ecc.).

d) **Continuità di azione**

L'Organismo di Vigilanza deve poter svolgere in modo continuativo le attività necessarie per la vigilanza del Modello, con adeguato impegno e con i necessari poteri di indagine. A tal fine, la continuità di azione è favorita dalla presenza di una struttura:

- dedicata esclusivamente all'attività di vigilanza del Modello di Organizzazione
- priva di mansioni operative, che possano portarla ad assumere decisioni con effetti economici-finanziari.

16.3 Requisiti Soggettivi dei Componenti l'Organismo di Vigilanza

Oltre ad essere qualificati professionalmente per poter svolgere efficacemente l'attività assegnata, ovvero avere in base al ruolo ricoperto competenza in relazione alle attività ispettive, di analisi dei sistemi di controllo, di tipo giuridico e più in particolare penalistico, i componenti dell'Organismo di Vigilanza all'atto della nomina e per tutta la durata dell'incarico non devono:

a) aver riportato sentenze di condanna (o patteggiamento), anche non definitive per un reato, incluse le sentenze che comportano l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi, o l'inabilitazione, né devono essere stati dichiarati falliti o, comunque, aver riportato una condanna per uno dei reati previsti dal Decreto
b) avere relazioni di parentela o affinità entro il quarto grado con i membri del Consiglio di Amministrazione o del Collegio Sindacale della Società, nonché con i medesimi membri delle società controllanti e/o eventualmente controllate o con i soggetti esterni incaricati della revisione
c) avere rapporti di natura patrimoniale con i componenti e la Società o le società che la controllano o le società da questa controllate, tali da compromettere l'indipendenza dei componenti stessi
d) essere in conflitto di interesse con la Società.

16.4 Nomina e Cessazione dall'Incarico

L'incarico nell'Organismo di Vigilanza è conferito con Delibera del Consiglio di Amministrazione per la durata di 3 anni, fino al 20/12/2025. Con la medesima Delibera è nominato, tra i componenti dell'Organismo di Vigilanza, il Presidente identificato dagli stessi e sono determinate le risorse umane e materiali (budget) delle quali l'Organismo di Vigilanza può disporre autonomamente per esercitare la sua funzione.

La validità dell'incarico richiede l'accettazione formale dello stesso da parte dei soggetti incaricati.

L'Organo Amministrativo può riconoscere emolumenti ai membri dell'Organismo di Vigilanza. Ove riconosciuti, tali emolumenti dovranno essere stabiliti nell'atto di nomina o con successiva delibera dell'Organo amministrativo.

La cessazione dall'incarico dell'intero Organismo di Vigilanza può avvenire per una delle seguenti cause:

- **scadenza** dell'incarico
- **revoca** dell'Organismo di Vigilanza da parte del Consiglio di Amministrazione
- **rinuncia** dei componenti dell'Organismo di Vigilanza, formalizzata mediante apposita comunicazione scritta inviata al Consiglio di Amministrazione.

La **revoca** dell'Organismo di Vigilanza può avvenire solo per giusta causa, anche al fine di garantirne l'assoluta indipendenza. Al di fuori delle ipotesi riguardanti l'intero Organismo di Vigilanza, la cessazione dell'incarico del "singolo" componente può avvenire:

- a seguito di revoca dell'incarico da parte del Consiglio di Amministrazione
- a seguito di rinuncia all'incarico, formalizzata mediante apposita comunicazione scritta inviata al Consiglio di Amministrazione
- a seguito del verificarsi, nel corso dell'incarico, di una causa di ineleggibilità: in tal caso, il membro interessato è tenuto ad informare immediatamente gli altri componenti dell'Organismo di Vigilanza e il Consiglio di Amministrazione.

In caso di morte, **scadenza**, **revoca** o **rinuncia** di uno o più componenti, lo stesso Consiglio di Amministrazione delibera, entro sessanta giorni dalla notizia dell'evento, il/i membro/i sostitutivo/i.

Nelle more, ove possibile, l'Organismo di Vigilanza continua il suo operato con i componenti rimasti in carica. In caso di sostituzione o di impedimento del Presidente, la presidenza è assunta dal membro effettivo più anziano fino alla nomina del nuovo Presidente. Il ruolo di Presidente non può essere assunto del membro che riveste anche la carica di Sindaco. I nuovi nominati scadono alla scadenza di quelli già in carica.

La nomina dei componenti dell'Organismo di Vigilanza, così come la loro cessazione dall'ufficio, deve risultare dal verbale dell'Organo Amministrativo della Società, con i dati anagrafici di ogni membro, la qualifica professionale e la qualità di Presidente o Membro dell'Organismo di Vigilanza, così come pure le motivazioni circa la sussistenza dei requisiti di indipendenza, autonomia, onorabilità e professionalità per ciascuno di essi.

La composizione dell'Organismo di Vigilanza, i suoi compiti e i suoi poteri, sono comunicati all'organizzazione mediante la pubblicazione del presente documento e della Delibera del Consiglio di Amministrazione sulla rete intranet aziendale non appena interviene l'accettazione.

16.5 Compiti e Poteri dell'Organismo di Vigilanza

Le attività che l'Organismo di Vigilanza è chiamato ad assolvere sono:

- vigilare sul funzionamento e sull'osservanza del Modello di Organizzazione e Gestione, ovvero:
  - vigilare sull'effettività del Modello di Organizzazione e Gestione, attraverso la verifica della coerenza tra i comportamenti concretamente posti in essere all'interno della Società e il modello istituito
  - verificare l'adeguatezza e l'efficacia del Modello di Organizzazione e Gestione, ovvero la sua reale e non meramente formale capacità di prevenire i comportamenti illeciti
  - segnalare all'organo dirigente, per gli opportuni provvedimenti, quelle violazioni accertate che possano comportare l'insorgere di una responsabilità in capo alla Società

- analizzare il mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello di Organizzazione e Gestione
- promuovere iniziative per la formazione dei destinatari del Modello e per la sua comunicazione e diffusione, predisponendo la documentazione a ciò necessaria, coordinandosi con il soggetto incaricato della formazione e diffusione del Modello

- curare l'aggiornamento, ove necessario, del Modello di Organizzazione e Gestione, attraverso:
  - la definizione e la presentazione di proposte di adeguamento del Modello di Organizzazione e Gestione al Consiglio di Amministrazione o alle funzioni aziendali eventualmente competenti, nell'ipotesi in cui le analisi operate rendano necessario effettuare correzioni, integrazioni e adeguamenti, al fine di migliorarne l'adeguatezza e l'efficacia, anche in considerazione di eventuali sopraggiunti interventi normativi e/o di variazioni della struttura organizzativa o dell'attività aziendale e/o di riscontrate significative violazioni del Modello di Organizzazione e Gestione
  - lo svolgimento di follow up per accertare l'attuazione e l'effettiva funzionalità delle soluzioni proposte.

All'Organismo di Vigilanza sono riconosciuti tutti i poteri necessari ad assicurare una puntuale ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello di Organizzazione e Gestione, nessuno escluso. L'Organismo di Vigilanza ha facoltà:

- di effettuare, anche non annunciate, tutte le verifiche ritenute opportune ai fini del corretto espletamento dei propri compiti
- di libero accesso presso tutte le funzioni, gli archivi e i documenti della Società, senza alcun consenso preventivo o necessità di autorizzazione, al fine di ottenere ogni informazione, dato o documento ritenuto necessario per lo svolgimento dei suoi compiti
- richiedere e ottenere da parte di tutte le funzioni copia della documentazione aziendale di interesse, se del caso nel rispetto delle vie gerarchiche
- di disporre, ove occorra, della collaborazione delle risorse che possano fornire indicazioni o informazioni utili in merito allo svolgimento dell'attività aziendale o ad eventuali disfunzioni o violazioni del Modello di Organizzazione e Gestione
- di avvalersi, sotto la propria diretta sorveglianza e responsabilità, dell'ausilio di tutte le strutture della Società ovvero di consulenti esterni, segnalandone la necessità all'Organo Amministrativo
- di disporre, per le eventuali esigenze dettate dall'espletamento delle proprie funzioni, delle risorse finanziarie stanziate dal Consiglio di Amministrazione.

16.6 I Profili di Responsabilità dei Componenti dell'Organismo di Vigilanza

Secondo la normativa vigente, in capo all'Organismo di Vigilanza non grava l'obbligo, penalmente sanzionabile, di impedire la commissione dei reati indicati nel Decreto.

I membri dell'Organismo di Vigilanza possono considerarsi responsabili solo per eventuali omissioni nell'espletamento dell'incarico, responsabilità che non si estende al membro che abbia fatto annotare il proprio dissenso nei verbali delle riunioni dell'Organismo.

Tali omissioni sono causa di revoca dall'incarico.

16.7 Regole di Funzionamento dell'Organismo di Vigilanza

L'Organismo di Vigilanza ha il compito di vigilare sull'operato aziendale; a tal fine deve:

- provvedere alle deliberazioni di propria competenza
- definire annualmente il Piano di Attività
- favorire un adeguato flusso informativo con le strutture aziendali.

16.7.1 Convocazione e Deliberazione dell'Organismo di Vigilanza

Per quanto attiene, invece, alle regole di convocazione e deliberazione:

- l'Organismo di Vigilanza si riunisce periodicamente, su convocazione del Presidente
- l'Organismo di Vigilanza è presieduto dal suo Presidente: in caso di assenza o impedimento, il Presidente è sostituito dal componente più anziano nella carica o, in caso di parità, più anziano di età
- le funzioni di segreteria sono esercitate da uno dei componenti l'Organismo di Vigilanza, o da un ulteriore soggetto individuato dall'Organismo di Vigilanza, che redige il verbale di ciascuna seduta, sottoscritto da tutti i partecipanti
- per la validità delle sedute, è richiesto l'intervento della maggioranza dei membri in carica
- le decisioni sono assunte a maggioranza dei voti dei presenti; in caso di parità, prevale il voto del Presidente
- sono esclusi dal voto i membri dell'Organismo di Vigilanza, i quali dovessero trovarsi in situazioni di conflitto di interesse in relazione alle deliberazioni da assumere, pur essendo ammessi alla partecipazione alle discussioni.

16.7.2 Redazione e Realizzazione del Piano di Attività

Annualmente, nonchè ogni qualvolta risulti necessario, l'Organismo di Vigilanza deve verificare la mappa delle aree a rischio reato, al fine di adeguarla a eventuali mutamenti dell'attività e/o della struttura aziendale, ovvero ad aggiornamenti normativi.

Tali adeguamenti si sostanzieranno nell'aggiornamento e riemissione del documento di Analisi del Rischio.

A tal fine, all'Organismo di Vigilanza devono essere segnalate – da parte del management e degli addetti alle attività di controllo, nell'ambito delle singole funzioni – le eventuali situazioni che possono esporre l'Azienda al rischio di reati.

Tali comunicazioni devono essere esclusivamente scritte.

Le attività che l'Organismo di Vigilanza intende svolgere in attuazione del D.Lgs. 231/01, relativamente alle aree considerate maggiormente a rischio reato, sono riportate in un documento, denominato Piano di Attività dell'Organismo di Vigilanza, nel quale lo stesso provvede a:

- definire le attività ispettive che intende compiere nel corso dell'anno
- fornire una pianificazione temporale delle attività definite
- identificare le funzioni o processi coinvolti, nonché le informazioni che dovranno essere fornite all'Organismo di Vigilanza e le relative modalità e periodicità
- definire le necessarie risorse finanziarie (budget dell'Organismo di Vigilanza), strumentali e umane
- prevedere la pianificazione pluriennale degli interventi di verifica e di controllo.

16.7.3 Informazioni verso l'Organismo di Vigilanza

I flussi informativi che i Destinatari hanno l'obbligo di garantire nei confronti dell'Organismo di Vigilanza possono essere:

- periodici e appartenenti alla normale attività tipica del processo di controllo
- *ad hoc* e relativi a fattispecie peculiari, indicative di specifici rischi in essere.

Per quanto riguarda il contenuto dei primi, devono essere periodicamente comunicate per iscritto all'Organismo di Vigilanza:

- informazioni significative sulle attività svolte
- modifiche organizzative (ivi incluse quelle al sistema delle deleghe) e/o di business eventualmente intervenute
- modifiche procedurali eventualmente intervenute
- report in materia di salute e sicurezza sul lavoro
- report derivanti dall'attività di verifica effettuata dalla società di revisione.

L'Organismo di Vigilanza può richiedere, contestualmente alle informazioni contenute nei flussi, un'attestazione di conformità alle prescrizioni dettate dal Modello di Organizzazione e Gestione da parte del management: responsabilità del management è, infatti, anche quella di istituire un concreto processo di "auto-valutazione" del sistema di controllo interno. I flussi *ad hoc* destinati all'Organismo di Vigilanza sono relativi a criticità e possono riguardare:

- procedimenti posti in essere dalla Magistratura o da autorità pubbliche in relazione a reati previsti dal Decreto
- risultanze di indagini interne dalle quali sono emerse infrazioni del Modello di Organizzazione e Gestione
- procedimenti disciplinari a carico di dipendenti per infrazioni del Modello di Organizzazione e Gestione o del *Codice Etico*
- possibili violazioni del Modello di Organizzazione e Gestione (cd. segnalazioni)
- indici di anomalie tali che facciano ragionevolmente ipotizzare una violazione degli obblighi contenuti nel Modello
- profili problematici rilevanti sorti con riferimento all'applicazione dei presidi di controllo previsti dal Modello di Organizzazione e Gestione
- notizie relative all'effettiva attuazione del Modello a tutti i livelli aziendali, con evidenza – nell'ambito dei procedimenti disciplinari svolti – delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

Nel dettaglio, le informazioni e i relativi documenti che, in relazione a specifici eventi, devono essere notificati all'OdV, la funzione che deve trasmetterli e la relativa frequenza, sono definiti annualmente nel Piano di Attività sulla base delle risultanze della revisione e dell'eventuale aggiornamento delle aree a rischio reato.

Le informazioni e i relativi documenti devono essere inoltrati all'OdV attraverso il seguente indirizzo di posta elettronica:

odv_maticmind@legalmail.it

L'OdV cura la diffusione di specifiche istruzioni per facilitare il flusso di informazioni verso l'OdV e per risolvere velocemente casi di dubbio.

16.8 Gestione Segnalazioni da Parte dell'Organismo di Vigilanza

L'Organismo di Vigilanza deve essere informato in merito a violazione o sospetti di violazione del Modello di Organizzazione e Gestione, che potrebbero determinare responsabilità ai sensi del D.Lgs. 231/2001. Pertanto, deve essere portata a conoscenza dell'Organismo di Vigilanza ogni informazione, anche proveniente da terzi, attinente all'attuazione di quanto contemplato dal Modello di Organizzazione e Gestione. In particolare, secondo quanto trattato nella Procedura di Segnalazione Illeciti ed Irregolarità ed utilizzando la piattaforma di segnalazione messa a disposizione:

- devono essere trasmesse da ciascun Responsabile di Funzione eventuali segnalazioni relative alla commissione o al ragionevole pericolo di commissione dei reati contemplati dal Decreto o comunque a comportamenti in generale non in linea con le regole di comportamento di cui al Modello di Organizzazione e Gestione
- ciascun Dipendente, nel rispetto del *Codice Etico* aziendale, deve segnalare la violazione, anche presunta, del Modello di Organizzazione e Gestione
- anche i Consulenti e i Partner sono tenuti ad effettuare direttamente all'Organismo di Vigilanza la segnalazione di violazioni perpetrate o presunte, di cui sono venuti a conoscenza nel corso dello svolgimento della loro attività per Maticmind.

L'Organismo di Vigilanza deve essere informato anche di:

- eventuali comunicazioni delle società di revisione riguardanti aspetti che possono indicare carenze nel sistema dei controlli interni, fatti censurabili, osservazioni sul bilancio della Società
- dichiarazione di veridicità e completezza delle informazioni contenute nelle comunicazioni sociali.

Le segnalazioni dovranno essere in linea con quanto previsto dal presente documento e al *Codice Etico*, avere ad oggetto violazioni o sospetti di violazione del Modello di Organizzazione e Gestione ed essere inoltrate in forma scritta tramite la piattaforma di segnalazione residente nel sito ww.matimind.it all'indirizzo:

https://maticmind.whistlelink.com/

Le informazioni/segnalazioni vanno comunque trattate nel rispetto della legge sulla tutela della privacy, con le prescritte misure di sicurezza.

L'OdV cura la diffusione di specifiche istruzioni per facilitare il flusso di segnalazioni verso l'OdV e per risolvere velocemente casi di dubbio.

16.8.1 Metodologia di Trattamento delle Segnalazioni

Alla ricezione di una segnalazione l'Organismo di Vigilanza provvede a Supportare la Direzione Compliance:

- nel valutare le segnalazioni ricevute e le iniziative da porre in essere
- se necessario, ascoltare l'autore della segnalazione, nonché il presunto responsabile della violazione
- motivare per iscritto l'eventuale diniego all'indagine o l'archiviazione
- garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti delle società o delle persone accusate in mala fede.

Eventuali provvedimenti sanzionatori saranno adottati dagli organi e dagli Uffici societari competenti.

16.9 Riporto da Parte dell'OdV nei Confronti degli Organi Sociali

L'Organismo di Vigilanza è tenuto a:

- documentare puntualmente, anche mediante la compilazione e la tenuta di appositi registri, tutte le attività svolte, le iniziative e i provvedimenti adottati, così come le informazioni e le segnalazioni ricevute, anche al fine di garantire la completa tracciabilità degli interventi intrapresi
- documentare le indicazioni fornite alle funzioni aziendali interessate, ivi comprese quelle inerenti alla necessità di apportare modifiche all'Analisi del Rischio, al Modello di Organizzazione e Gestione o alle procedure operative derivanti da modifiche di legge o organizzative
- registrare e conservare tutta la documentazione formata, ricevuta o comunque raccolta nel corso del proprio incarico e rilevante ai fini del corretto svolgimento dell'incarico stesso
- informare e sensibilizzare il Consiglio di Amministrazione relativamente allo stato di implementazione del Modello di Organizzazione e Gestione
- assicurare il puntuale adempimento di tutte le attività di reporting inerenti al rispetto del Modello di Organizzazione e Gestione.

16.9.1 Reporting

L'attività di reporting ha ad oggetto, in particolare:

- l'attività, in genere, svolta dall'Organismo di Vigilanza
- eventuali problematiche o criticità che si siano evidenziate nel corso dell'attività di vigilanza
- le azioni correttive, necessarie o eventuali, da apportare al fine di assicurare l'efficacia e l'effettività del Modello di Organizzazione e Gestione, nonché lo stato di attuazione delle azioni correttive deliberate dal Consiglio di Amministrazione
- l'accertamento di comportamenti non in linea con il Modello di Organizzazione e Gestione
- la rilevazione di carenze organizzative o procedurali tali da esporre la Società al pericolo che siano commessi reati rilevanti ai fini del Decreto
- l'eventuale mancata o carente collaborazione da parte delle funzioni aziendali nell'espletamento dei propri compiti di verifica e/o d'indagine
- in ogni caso, qualsiasi informazione ritenuta utile ai fini dell'assunzione di determinazioni urgenti da parte degli organi deputati

In ogni caso, l'Organismo di Vigilanza può rivolgersi al Consiglio di Amministrazione ogni qualvolta lo ritenga opportuno ai fini dell'efficace ed efficiente adempimento dei compiti ad esso assegnati.

Gli incontri dell'OdV sono verbalizzati e le copie dei verbali conservate.
L'Organismo di Vigilanza relaziona almeno una volta l'anno per iscritto:

- l'Assemblea dei Soci
- il Consiglio di Amministrazione
- il Collegio Sindacale

sull'attività compiuta nel periodo, ivi incluse le informazioni circa i reati che si fossero eventualmente verificati, le presunte violazioni del Modello e/o le segnalazioni ricevute, nonché il rendiconto relativo alle modalità di impiego delle risorse finanziarie costituenti il budget in dotazione all'Organismo di Vigilanza e sull'esito della stessa attività, fornendo una pianificazione di massima sulle aree di intervento per il periodo successivo.

16.9.2 Archiviazione della Documentazione dell'Organismo di Vigilanza

Ogni verbale, informazione, documentazione, segnalazione previsti nel Modello di Organizzazione e Gestione sono conservati dall'Organismo di Vigilanza.

I Verbali delle sedute dell'Organismo di Vigilanza sono riportati nel "*Libro Verbali dell'Organismo di Vigilanza*" a firma del Presidente e di un componente in funzione anche di Segretario, scelto dall'Organismo di Vigilanza.

I documenti ricevuti dall'Organismo di Vigilanza o da questo inviati alle varie funzioni, nonché i verbali di ciascuna seduta dell'Organismo di Vigilanza redatti dalla funzione di segreteria e sottoscritti dai partecipanti sono archiviati dall'Organismo di Vigilanza stesso per la durata di 10 anni o, se superiore, per il periodo previsto dalle specifiche disposizioni di legge vigenti.

I dati e le informazioni conservate nel database sono posti a disposizione di soggetti esterni all'Organismo di Vigilanza, che possano averne diritto, previa autorizzazione dell'Organismo stesso e con immediata informazione all'Organo Amministrativo e al Collegio Sindacale di Maticmind.

17 ALLEGATO 1 - CROSS MAP: REATI-DOCUMENTAZIONE

Reato presupposto	Documenti di riferimento
Indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello stato o di un ente pubblico	
Truffa in danno dello Stato o di altro Ente Pubblico	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ750_2_Gestione Documenti di Registrazione della Qualita
	MM_MOD231_Codice Etico
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
Frode informatica in danno dello Stato o di altro Ente Pubblico	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ750_2_Gestione Documenti di Registrazione della Qualita
	MM_MOD231_Codice Etico
	MM_SGSI_PR005_Procedura Sicurezza Logica
	MM_SGSI_P005_Politica di Sicurezza Logica
	MM_SGSI_P003_Politica Gestione Sicurezza Rapporti Terze Parti
	MM_GDPR_P003 Procedura gestione delle nomine AdS
	Procedura Sicurezza Logica Cliente
	Politica Sicurezza Logica Cliente
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
Delitti informatici e trattamento illecito di dati	
Falsità in un documento informatico pubblico o avente efficacia probatoria	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ750_2_Gestione Documenti di Registrazione della Qualita
	MM_MOD231_Codice Etico
	MM_Manuale Operativo SIM Presales
Accesso abusivo ad un sistema informatico o telematico	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ750_2_Gestione Documenti di Registrazione della Qualita
	MM_SGSI_PR005_Procedura Sicurezza Logica
	MM_SGSI_P005_Politica di Sicurezza Logica
	MM_SGSI_P003_Politica Gestione Sicurezza Rapporti Terze Parti
	MM_GDPR_P003 Procedura gestione delle nomine AdS
	Procedura Sicurezza Logica Cliente
	Politica Sicurezza Logica Cliente
	MM_PAQ840_1_Gestione dei Fornitori
	MM_MOD231_Codice Etico
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	MM_SGSI_PR005_Procedura Sicurezza Logica

Reato presupposto	Documenti di riferimento
	MM_SGSI_P005_Politica di Sicurezza Logica
	MM_SGSI_P003_Politica Gestione Sicurezza Rapporti Terze Parti
	MM_PAQ840_1_Gestione dei Fornitori
	Procedura Sicurezza Logica Cliente
	Politica Sicurezza Logica Cliente
	MM_MOD231_Codice Disciplinare
	MM_MOD231_Codice Etico
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ851_13_CCA_Gestione Project Management
	MM_PAQ852_2_CCA_Gestione della Configurazione
	MM_SGI_Piano di Gestione della Configurazione
	MM_PAQ851_12_Gestione Attività di Delivery
	MM_PAQ851_12_Gestione Service Operation
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_SGSI_PR005_Procedura Sicurezza Logica
	MM_SGSI_P005_Politica di Sicurezza Logica
	MM_SGSI_P003_Politica Gestione Sicurezza Rapporti Terze Parti
	MM_GDPR_P003 Procedura gestione delle nomine AdS
	Procedura Sicurezza Logica Cliente
	Politica Sicurezza Logica Cliente
	Modulo Intervento Tecnico (MIT) firmato dal Cliente
	Verbale di Collaudo firmato dal Cliente
	MM_MOD231_Codice Disciplinare
	MM_MOD231_Codice Etico
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ851_13_CCA_Gestione Project Management
	MM_PAQ852_2_CCA_Gestione della Configurazione
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_12_Gestione Attività di Delivery
	MM_PAQ851_12_Gestione Service Operation
	MM_PAQ854_1_Gestione del Magazzino
	MM_SGSI_PR005_Procedura Sicurezza Logica
	MM_SGSI_P005_Politica di Sicurezza Logica
	MM_SGSI_P003_Politica Gestione Sicurezza Rapporti Terze Parti
	MM_GDPR_P003 Procedura gestione delle nomine AdS
	Procedura Sicurezza Logica Cliente
	Politica Sicurezza Logica Cliente
	Modulo Intervento Tecnico (MIT) firmato dal Cliente

Reato presupposto	Documenti di riferimento
	Verbale di Collaudo firmato dal Cliente
	MM_Manuale Operativo SIM Presales
	MM_MOD231_Codice Disciplinare
	MM_MOD231_Codice Etico
Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ851_13_CCA_Gestione Project Management
	MM_PAQ852_2_CCA_Gestione della Configurazione
	MM_SGI_Piano di Gestione della Configurazione
	MM_PAQ851_12_Gestione Attività di Delivery
	MM_PAQ851_12_Gestione Service Operation
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ854_1_Gestione del Magazzino
	MM_SGSI_PR005_Procedura Sicurezza Logica
	MM_SGSI_P005_Politica di Sicurezza Logica
	MM_SGSI_P003_Politica Gestione Sicurezza Rapporti Terze Parti
	MM_GDPR_P003 Procedura gestione delle nomine AdS
	Procedura Sicurezza Logica Cliente
	Politica Sicurezza Logica Cliente
	Modulo Intervento Tecnico (MIT) firmato dal Cliente
	Verbale di Collaudo firmato dal Cliente
	MM_Manuale Operativo SIM Presales
	MM_MOD231_Codice Etico
Danneggiamento di informazioni, dati e programmi informatici	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ851_13_CCA_Gestione Project Management
	MM_PAQ852_2_CCA_Gestione della Configurazione
	MM_SGI_Piano di Gestione della Configurazione
	MM_PAQ851_12_Gestione Attività di Delivery
	MM_PAQ851_12_Gestione Service Operation
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ854_1_Gestione del Magazzino
	MM_SGSI_PR005_Procedura Sicurezza Logica
	MM_SGSI_P005_Politica di Sicurezza Logica
	MM_SGSI_P003_Politica Gestione Sicurezza Rapporti Terze Parti
	MM_GDPR_P003 Procedura gestione delle nomine AdS
	Procedura Sicurezza Logica Cliente
	Politica Sicurezza Logica Cliente
	Modulo Intervento Tecnico (MIT) firmato dal Cliente
	Verbale di Collaudo firmato dal Cliente
	MM_Manuale Operativo SIM Presales
	MM_MOD231_Codice Disciplinare

Reato presupposto	Documenti di riferimento
	MM_MOD231_Codice Etico
Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ851_13_CCA_Gestione Project Management
	MM_PAQ852_2_CCA_Gestione della Configurazione
	MM_SGI_Piano di Gestione della Configurazione
	MM_PAQ851_12_Gestione Attività di Delivery
	MM_PAQ851_12_Gestione Service Operation
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ854_1_Gestione del Magazzino
	MM_SGSI_PR005_Procedura Sicurezza Logica
	MM_SGSI_P005_Politica di Sicurezza Logica
	MM_SGSI_P003_Politica Gestione Sicurezza Rapporti Terze Parti
	MM_GDPR_P003 Procedura gestione delle nomine AdS
	Procedura Sicurezza Logica Cliente
	Politica Sicurezza Logica Cliente
	Modulo Intervento Tecnico (MIT) firmato dal Cliente
	Verbale di Collaudo firmato dal Cliente
	MM_Manuale Operativo SIM Presales
	MM_MOD231_Codice Disciplinare
	MM_MOD231_Codice Etico
Danneggiamento di sistemi informatici o telematici	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ851_13_CCA_Gestione Project Management
	MM_PAQ852_2_CCA_Gestione della Configurazione
	MM_SGI_Piano di Gestione della Configurazione
	MM_PAQ851_12_Gestione Attività di Delivery
	MM_PAQ851_12_Gestione Service Operation
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ854_1_Gestione del Magazzino
	MM_SGSI_PR005_Procedura Sicurezza Logica
	MM_SGSI_P005_Politica di Sicurezza Logica
	MM_SGSI_P003_Politica Gestione Sicurezza Rapporti Terze Parti
	MM_GDPR_P003 Procedura gestione delle nomine AdS
	Procedura Sicurezza Logica Cliente
	Politica Sicurezza Logica Cliente
	Modulo Intervento Tecnico (MIT) firmato dal Cliente
	Verbale di Collaudo firmato dal Cliente
	MM_Manuale Operativo SIM Presales
	MM_MOD231_Codice Disciplinare
	MM_MOD231_Codice Etico
Danneggiamento di sistemi informatici o telematici di pubblica utilità	MM_PAQ820_2_Gestione Ordine di Vendita

Reato presupposto	Documenti di riferimento
	MM_PAQ851_13_CCA_Gestione Project Management
	MM_PAQ852_2_CCA_Gestione della Configurazione
	MM_SGI_Piano di Gestione della Configurazione
	MM_PAQ851_12_Gestione Attività di Delivery
	MM_PAQ851_12_Gestione Service Operation
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ854_1_Gestione del Magazzino
	MM_SGSI_PR005_Procedura Sicurezza Logica
	MM_SGSI_P005_Politica di Sicurezza Logica
	MM_SGSI_P003_Politica Gestione Sicurezza Rapporti Terze Parti
	Procedura Sicurezza Logica Cliente
	Politica Sicurezza Logica Cliente
	Modulo Intervento Tecnico (MIT) firmato dal Cliente
	Verbale di Collaudo firmato dal Cliente
	MM_Manuale Operativo SIM Presales
	MM_MOD231_Codice Disciplinare
	MM_MOD231_Codice Etico
Delitti di criminalità organizzata	
Associazione per delinquere	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ840_1_Gestione dei Fornitori
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_MOD231_Codice Etico
Associazione di tipo mafioso	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ840_1_Gestione dei Fornitori
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_MOD231_Codice Etico
Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_MOD231_Codice Disciplinare
	MM_MOD231_Codice Etico

Reato presupposto	Documenti di riferimento
Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_MOD231_Codice Etico
Illegale fabbricazione, introduzione nello Stato, vendita, detenzione e porto in luogo pubblico di armi da guerra	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_MOD231_Codice Etico
Concussione e corruzione	
Concussione	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ820_4_Procedura di gestione di regali e viaggi
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_Manuale Operativo Ztravel_Gestione Trasferte
	MM_Manuale Operativo Ztravel_Gestione Note Spese
	MM_MOD231_Codice Etico
Corruzione per l'esercizio della funzione	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_11_Contract Management
	MM_PAQ820_4_Procedura di gestione di regali e viaggi
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_Manuale Operativo Ztravel_Gestione Trasferte
	MM_Manuale Operativo Ztravel_Gestione Note Spese
	MM_MOD231_Codice Etico
Corruzione per un atto contrario ai doveri d'ufficio	MM_PAQ820_1_Progettazione Offerta di Vendita

Reato presupposto	Documenti di riferimento
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_11_Contract Management
	MM_PAQ820_4_Procedura di gestione di regali e viaggi
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_Manuale Operativo Ztravel_Gestione Trasferte
	MM_Manuale Operativo Ztravel_Gestione Note Spese
	MM_MOD231_Codice Etico
Corruzione in atti giudiziari	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_11_Contract Management
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_Manuale Operativo Ztravel_Gestione Trasferte
	MM_Manuale Operativo Ztravel_Gestione Note Spese
	MM_MOD231_Codice Etico
Induzione indebita a dare o promettere utilità	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_11_Contract Management
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_Manuale Operativo Ztravel_Gestione Trasferte
	MM_Manuale Operativo Ztravel_Gestione Note Spese
	MM_MOD231_Codice Etico
Corruzione di persona incaricata di un pubblico servizio	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_11_Contract Management
	MM_PAQ820_4_Procedura di gestione di regali e viaggi
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision

Reato presupposto	Documenti di riferimento
	MM_Manuale Operativo Ztravel_Gestione Trasferte
	MM_Manuale Operativo Ztravel_Gestione Note Spese
	MM_MOD231_Codice Etico
Pene per il corruttore	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_11_Contract Management
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_Manuale Operativo Ztravel_Gestione Trasferte
	MM_Manuale Operativo Ztravel_Gestione Note Spese
	MM_MOD231_Codice Etico
Istigazione alla corruzione	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_11_Contract Management
	MM_PAQ820_4_Procedura di gestione di regali e viaggi
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_Manuale Operativo Ztravel_Gestione Trasferte
	MM_Manuale Operativo Ztravel_Gestione Note Spese
	MM_MOD231_Codice Etico
Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_11_Contract Management
	MM_PAQ820_4_Procedura di gestione di regali e viaggi
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_Manuale Operativo Ztravel_Gestione Trasferte
	MM_Manuale Operativo Ztravel_Gestione Note Spese
	MM_MOD231_Codice Etico
Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento	

Reato presupposto	Documenti di riferimento
Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_12_Gestione del Service_Management
	MM_PAQ851_11_Gestione Hardware Team
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
Introduzione nello Stato e commercio di prodotti con segni falsi	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_12_Gestione del Service_Management
	MM_PAQ851_11_Gestione Hardware Team
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
Reati societari	
False comunicazioni sociali	MM_MOD231_Codice Etico
Impedito controllo	MM_MOD231_Codice Etico
Indebita restituzione di conferimenti	MM_MOD231_Codice Etico
Illegale ripartizione degli utili e delle riserve	MM_MOD231_Codice Etico
Illecite operazioni su azioni o quote sociali o di società controllante	MM_MOD231_Codice Etico
Operazioni in pregiudizio dei creditori	MM_MOD231_Codice Etico
Formazione fittizia del capitale	MM_MOD231_Codice Etico
Corruzione tra privati	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_11_Contract Management
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_Manuale Operativo Ztravel_Gestione Trasferte
	MM_Manuale Operativo Ztravel_Gestione Note Spese
	MM_MOD231_Codice Etico
Delitti contro la personalità individuale	
Pornografia minorile	MM_MOD231_Codice Etico
Detenzione di materiale pornografico	MM_MOD231_Codice Etico

Reato presupposto	Documenti di riferimento
Pornografia virtuale	MM_MOD231_Codice Etico
Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro	
Omicidio colposo	MM_20191002_PAQ812_1_Gestione Sicurezza negli Appalti
	07_01_09_VERBALI E COMUNICAZIONI (documentazione)
	MM_20191002_8108_DVR TOMO 1_Luoghi_di_Lavoro
	MM_20191002_8108_DVR TOMO 2_Mansionario_v3.0
	MM_20191002_8108_DVR_TOMO_3_0_Luoghi_di_Lavoro_Extra_Sede
	MM_20191002_PAQ812_1_Gestione Sicurezza negli Appalti
	MM_2020516_8108_ODS_SARSCOV2
	MM_20200516_8108_GCP_SARSCOV2
	MM_20200516_8108_DVR_TOMO_3_ ALL_I_Rischio_Biologico_SARSCOV2
	MM_MOD231_Codice Etico
Lesioni personali colpose	MM_20191002_PAQ812_1_Gestione Sicurezza negli Appalti
	07_01_09_VERBALI E COMUNICAZIONI (documentazione)
	MM_20191002_8108_DVR TOMO 1_Luoghi_di_Lavoro
	MM_20191002_8108_DVR TOMO 2_Mansionario_v3.0
	MM_20191002_8108_DVR_TOMO_3_0_Luoghi_di_Lavoro_Extra_Sede
	MM_20191002_PAQ812_1_Gestione Sicurezza negli Appalti
	MM_2020516_8108_ODS_SARSCOV2
	MM_20200516_8108_GCP_SARSCOV2
	MM_20200516_8108_DVR_TOMO_3_ ALL_I_Rischio_Biologico_SARSCOV2
	MM_MOD231_Codice Etico
Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita	
Ricettazione	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_MOD231_Codice Etico
Riciclaggio	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_MOD231_Codice Etico
Impiego di denaro, beni o utilità di provenienza illecita	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita

Reato presupposto	Documenti di riferimento
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_MOD231_Codice Etico
Autoriciclaggio	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_Manuale Operativo SIM Presales
	MM_Manuale Operativo Navision
	MM_MOD231_Codice Etico
Delitti in materia di violazione del diritto d'autore	
Messa a disposizione del pubblico in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, e senza averne diritto di un'opera o di parte di un'opera dell'ingegno protetta	MM_PAQ820_1_Progettazione Offerta di Vendita
	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_PAQ840_2_Gestione degli Approvvigionamenti
	MM_PAQ854_1_Gestione del Magazzino
	MM_Manuale Operativo SIM Presales
	MM_PAQ851_12_Gestione del Service_Management
	MM_PAQ851_12_Gestione Service Operation
	MM_IO720_1_Gestione Smart Licensing CISCO
	MM_PAQ851_11_Gestione Hardware Team
	Modulo Intervento Tecnico (MIT) firmato dal Cliente
	Verbale di Collaudo firmato dal Cliente
	MM_Manuale Operativo Configurazione Dispositivi Mobili
	MM_MOD231_Codice Etico
Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale ovvero concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi di protezione di programmi per elaboratori	MM_PAQ820_2_Gestione Ordine di Vendita
	MM_IO720_1_Gestione Smart Licensing CISCO
	MM_SGSI_PR005_Procedura Sicurezza Logica
	MM_SGSI_P005_Politica di Sicurezza Logica
	MM_SGSI_P003_Politica Gestione Sicurezza Rapporti Terze Parti
	MM_GDPR_P003 Procedura gestione delle nomine AdS
	Procedura Sicurezza Logica Cliente
	Politica Sicurezza Logica Cliente

Reato presupposto	Documenti di riferimento
	MM_MOD231_Codice Etico
Delitti in materia ambientale	
Attività di gestione di rifiuti non autorizzata	MM_MOD231_Codice Etico
Traffico illecito di rifiuti	MM_MOD231_Codice Etico
Attività organizzate per il traffico illecito di rifiuti	MM_MOD231_Codice Etico
Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	
Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_11_Contract Management
	MM_PAQ712_1_Gestione delle Risorse Umane
	MM_20200301_Gestione Documenti Presidio
	MM_20180926_Gestione Documenti Subappalto
	MM_MOD231_Codice Etico
Definizione di reato transnazionale	MM_PAQ840_1_Gestione dei Fornitori
	MM_PAQ851_11_Contract Management
	MM_PAQ712_1_Gestione delle Risorse Umane
	MM_20200301_Gestione Documenti Presidio
	MM_20180926_Gestione Documenti Subappalto
	MM_MOD231_Codice Etico