MODELLO DI ORGANIZZAZIONE E GESTIONE EX D.LGS. 231/2001

- PARTE SPECIALE -

Adottato con delibera del Consiglio di amministrazione del 27 marzo 2026

INDICE

PREMESSA

La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo adottato da Maticmind S.p.A. (qui di seguito "Maticmind" o la "Società") è stata redatta con l'obiettivo di tradurre in termini operativi e pratici il sistema di prevenzione dei reati previsto dal D. Lgs. 231/2001. In particolare, la presente Parte Speciale è finalizzata a identificare e disciplinare in modo puntuale tutte le attività aziendali che, per la loro natura o per le modalità con cui vengono svolte, potrebbero esporre la Società al rischio di commissione dei cd. Reati Presupposto rilevanti ai sensi della normativa citata.

La Parte Speciale è strutturata in Sezioni, ciascuna delle quali è dedicata a un'Area di Rischio specifica ed ai relativi Processi. Si è scelto di seguire questa impostazione perché ogni Area di Rischio rappresenta un insieme coerente di Processi che hanno caratteristiche, criticità e responsabilità gestionali comuni. Analizzare i rischi reato "per processo" consente di intervenire in modo più mirato e concreto nella prevenzione oltre che di rendere più fruibile il Modello ai Destinatari.

Per ciascun Processo vengono innanzitutto individuate le Attività Sensibili, ossia quelle attività che, se svolte in modo scorretto, opaco o disattento, potrebbero determinare un rischio penale.

I Reati Presupposto indicati per ciascuna Area di Rischio sono stati determinati all'esito del risk assessment condotto sulla Società[1].

Al fine di rendere ogni Sezione più comprensibile, sono indicati alcuni esempi di potenziali condotte penalmente rilevanti che potrebbero verificarsi in relazione alle Aree di Rischio.

Seguono poi i principi generali di condotta che tutti i Destinatari del Modello sono tenuti a osservare: si tratta di regole trasversali ispirate a criteri di legalità, trasparenza, correttezza, tracciabilità e collaborazione, pensate per orientare i comportamenti quotidiani e prevenire condotte illecite o irresponsabili.

A supporto, integrazione ed implementazione di questi principi, vengono richiamati i protocolli di condotta specifici e le procedure specifiche adottati da Maticmind per ciascuna Area di Rischio.

Si precisa che nella presente Parte Speciale:

- alcune procedure adottate dalla Società sono soltanto menzionate con rinvio integrale alla procedura di riferimento, in quanto il loro contenuto è altamente tecnico e difficilmente integrabile;
- alcune Sezioni non riportano protocolli di condotta specifici poiché i Processi ivi analizzati sono più esaustivamente coperti dalle procedure specifiche ad essi applicabili;

Per una descrizione integrale dei reati rilevanti si rimanda all'Allegato A del Modello; il sistema di flussi informativi verso l'Organismo di Vigilanza (OdV) è invece descritto integralmente nell'Allegato B del Modello.

[1] Con riferimento all'art. 25 D.Lgs. 231/2001, sono stati indicati solo i Reati Presupposto applicabili alla Società, ossia corruzione e traffico di influenze illecite.

1 SEZIONE 1: GESTIONE AMMINISTRATIVA E FINANZIARIA

PROCESSI	ATTIVITÀ SENSIBILI	FUNZIONE COINVOLTA	REATI PRESUPPOSTO RILEVANTI
Gestione delle risorse finanziarie	- Decisioni di spesa strategica e operativo-gestionale - Pianificazione finanziaria a medio/lungo termine - Movimentazione fondi tra conti - Riconciliazioni bancarie	- CFO - Direzione Finance: o Administration & Tax o Finance & Treasury o Budgeting & Control o Subsidiaries Finance Coordination o Ufficio Amministrazion e Banche - Amministratore Delegato - RU - Direzione Vendite	- Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24) - Reati informatici (art. 24 bis) - Delitti di criminalità organizzata (art. 24 ter) e reati transnazionali (L. 146/2006) - Corruzione e traffico di influenze illecite (art. 25) - Reati societari (art. 25 ter) - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio (art. 25 octies) - Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25 octies 1) - Reati in materia di violazione di misure restrittive dell'Unione Europea (art. 25 octies.2) - Reati tributari (art. 25 quinquiesdecies)
Tesoreria (cassa, carte aziendali, fondi spese, accordi infragruppo)	- Prelievo e deposito di fondi - Gestione carte prepagate o di credito aziendali - Rimborsi spese - Custodia fondi cassa - Gestione piccola cassa - Apertura e/o chiusura e gestione dei conti bancari - Riconciliazione degli estratti conto bancari - Rapporti finanziari infragruppo		
Operazioni di finanziamento	- Richiesta di finanziamenti agevolati o contributi pubblici - Predisposizione della documentazione di rendicontazione - Comunicazioni a enti erogatori		
Relazioni con banche, assicurazioni e altri intermediari finanziari	- Apertura/chiusura di conti correnti e strumenti finanziari - Gestione affidamenti e rapporti creditizi - Sottoscrizione di contratti finanziari		

1.1 Alcuni esempi dei Reati Presupposto rilevanti nella Gestione Amministrativa e Finanziaria

Si riportano qui di seguito, a titolo esemplificativo, alcune delle potenziali condotte penalmente rilevanti nell'ambito delle Attività Sensibili sopra menzionate:

a) Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24)

   - soggetti operanti in nome e/o per conto di Maticmind presentano documentazione falsa per ottenere fondi pubblici destinati a ricerca e sviluppo o innovazione tecnologica, in realtà indirizzati verso finalità diverse.

b) Reati in materia di violazione di misure restrittive dell'Unione europea (art. 25 octies 2)

   - soggetti operanti in nome e/o per conto di Maticmind effettuano triangolazioni per aggirare le misure restrittive imposte alla Russia e trasferire fondi a soggetti sanzionati.

c) Reati societari (art. 25 ter)

   - soggetti operanti in nome e/o per conto di Maticmind manipolano i dati del bilancio per nascondere perdite, sovrastimare i crediti o simulare ricavi, allo scopo di ottenere finanziamenti, migliorare il risultato dell'azienda o creare fondi neri.

1.2 Le regole generali di condotta nella Gestione Amministrativa e Finanziaria

I Destinatari della presente Parte Speciale devono:

- rispettare la normativa civilistica, penale, fiscale e di settore applicabile alla gestione finanziaria, nonché i principi contabili di riferimento;
- adottare comportamenti trasparenti e verificabili nella gestione delle risorse finanziarie, evitando ogni forma di opacità, irregolarità o artificio contabile;
- gestire i rapporti con banche, assicurazioni e altri intermediari finanziari nel rispetto della normativa antiriciclaggio, del principio di tracciabilità e dei poteri autorizzativi previsti;
- garantire che ogni operazione economica o finanziaria sia tracciabile, documentata, giustificata e autorizzata, in conformità ai livelli di responsabilità organizzativa;
- impegnarsi a non utilizzare, ricevere o movimentare fondi aziendali per finalità diverse da quelle istituzionali, né per fini personali, né per conto di terzi non autorizzati;
- evitare rapporti economici con soggetti la cui affidabilità o trasparenza non sia stata verificata, in particolare se localizzati in giurisdizioni a rischio o soggette a misure restrittive;
- impegnarsi a non creare contabilità parallele, fondi neri o conti non ufficiali, né attivare meccanismi di elusione dei controlli;

- impegnarsi a non effettuare operazioni in contanti se non per il caso di pagamenti per piccola cassa, consentiti per spese minute di importo massimo predefinito, sempre nel rispetto delle soglie di legge;
- impegnarsi a non effettuare trasferimenti di denaro tra conti correnti che non siano adeguatamente giustificati da operazioni commerciali, o eseguire pagamenti per prestazioni e servizi che non siano stati effettivamente resi o erogati;
- custodire e gestire con correttezza gli strumenti di pagamento elettronici aziendali (carte, token, conti online, app), evitando utilizzi impropri o fraudolenti;
- conoscere e applicare le procedure aziendali di budget, cassa, pagamenti, contabilità e investimenti, contribuendo al loro miglioramento continuo;
- favorire un sistema di controllo interno efficace e trasparente, supportando l'attività di monitoraggio dei rischi finanziari.

Con riferimento ai rapporti infragruppo, la Società vieta comportamenti che potrebbero, direttamente o indirettamente, integrare illeciti, quali, a titolo esemplificativo e non esaustivo:

- effettuare trasferimenti di denaro tra conti correnti delle società correlate che non siano adeguatamente giustificati da operazioni di natura finanziaria o commerciale o da eventuali contratti/accordi/convenzioni stipulati tra le parti;
- eseguire pagamenti per prestazioni e servizi che non siano stati effettivamente resi o erogati ovvero pagamenti in contanti o con mezzi non tracciabili del corrispettivo delle operazioni intercompany.

Fermo restando tali divieti, la Società:

- assicura che i rapporti infragruppo siano gestiti nel rispetto dei principi di reciproca autonomia gestionale, organizzativa e operativa nonché di correttezza, trasparenza, effettività e di separazione patrimoniale, anche al fine di garantire la tutela degli stakeholder di tutte le società correlate;
- vieta comportamenti che risultino pregiudizievoli per l'integrità o l'immagine di una delle società correlate; chiede che nessuna delle proprie partecipate ponga in essere comportamenti e/o adotti decisioni che, pur determinando benefici a proprio favore, potrebbero risultare pregiudizievoli per l'integrità o l'immagine di Maticmind.

La Società assicura inoltre che:

- i rapporti negoziali con le società correlate possano essere intrattenuti esclusivamente per iscritto da soggetti cui sia stato formalmente conferito incarico o autorizzazione in tal senso;
- siano individuati i criteri di determinazione dei corrispettivi per le prestazioni rese o ricevute da applicare alle operazioni commerciali e/o finanziarie intercompany;
- l'iter decisionale relativo a ciascuna operazione infragruppo avvenga in modo trasparente e tracciato con il coinvolgimento delle funzioni aziendali competenti per materia.

Tutte le operazioni infragruppo devono:

- rispondere a esigenze di razionalizzazione ed efficienza delle attività delle parti coinvolte;

- essere regolate a condizioni di mercato e, comunque, sulla base di valutazioni di reciproca convenienza economica e nel rispetto del principio di libera concorrenza;
- avvenire secondo criteri di correttezza sostanziale con chiara individuazione di ruoli e responsabilità nonché – nel rispetto dei principi di inerenza, congruità e certezza – dell'oggetto, delle modalità di esecuzione e dell'esatto corrispettivo;
- essere opportunamente motivate e sottoposte ad autorizzazione da parte di soggetti dotati di specifici poteri;
- prevedere che la prestazione, oggetto dell'operazione intercompany, avvenga in accordo con la normativa vigente, anche attraverso la previsione di penali e/o specifiche clausole che impongano il rispetto dei principi stabiliti nel Modello e nel Codice Etico;
- essere oggetto di verifica in ordine alla effettività del bene ceduto o del servizio reso o prestato e all'osservanza e al rispetto delle condizioni e delle modalità pattuite, e della normativa di riferimento, anche in materia fiscale.

1.3 I protocolli di condotta specifici

Gestione delle risorse finanziarie e della tesoreria

La Direzione Finance è guidata dal CFO e presidia la redazione dei documenti contabili, controlla i flussi finanziari e verifica l'allocazione delle risorse economiche e finanziarie, oltre a seguire le operazioni di budget e la contabilità generale e analitica.

Le attività specifiche relative alla Tesoreria e alla gestione finanziaria sono svolte principalmente dall'Ufficio Amministrazione Banche e dalla funzione Finance & Treasury.

L'Ufficio Amministrazione Banche si occupa della pianificazione finanziaria e della gestione dei rapporti con gli Istituti di Credito presso i quali l'azienda detiene i propri conti correnti.

Gestione dei conti correnti

La Società assicura:

- un'opportuna analisi di rischio-rendimento e di affidabilità/onorabilità dei possibili istituti di credito/finanziari con cui instaurare nuovi rapporti;
- che l'istituzione di nuovi rapporti o la dismissione di rapporti in essere con istituti bancari o finanziari sia opportunamente motivata e autorizzata, in conformità alle procedure vigenti;
- che le operazioni di apertura/chiusura di conti correnti, di giroconto, nonché la destinazione dei fondi in essi contenuti, la richiesta di fidi, fidejussioni e altre operazioni anche di natura straordinaria siano opportunamente motivate e autorizzate, in conformità alle disposizioni vigenti;

- nell'ambito delle periodiche attività di riconciliazione bancaria e di monitoraggio conti, la comunicazione tempestiva alle funzioni interessate di eventuali anomalie o discordanze riscontrate per la definizione delle opportune azioni da intraprendere;
- che l'accesso all'home banking sia consentito solo a soggetti che debbano avervi accesso in ragione della propria funzione e in ogni caso sotto supervisione, o revisione a posteriori, di funzioni apicali.

La gestione dei conti correnti è sotto la responsabilità dell'Ufficio Amministrazione Banche.

L'Ufficio esegue le attività di scarico giornaliero dei movimenti bancari dall'home banking e la riconciliazione dei saldi bancari.

La delega di potere per l'apertura, la modifica e l'estinzione di conti bancari e postali è stata conferita al Direttore Generale/Amministratore Delegato.

Per quanto riguarda i bonifici e i pagamenti, valgono i seguenti livelli autorizzativi:

- per importi fino a €5.000.000, i bonifici e i pagamenti richiedono la firma congiunta del Direttore Generale/Amministratore Delegato e di procuratori speciali;
- il limite massimo per singola disposizione di pagamento con la firma congiunta è di €20.000.000;
- i bonifici e i pagamenti di tasse, imposte, contributi o stipendi possono essere effettuati senza limite di importo.

Le procedure di gestione delle risorse finanziarie prevedono controlli finanziari e non finanziari per prevenire il rischio di corruzione e riciclaggio, basati sulla tracciabilità dei flussi finanziari e sull'imputazione di pagamento (titolo giustificativo).

Carte di credito o prepagate

L'uso e la gestione delle carte di credito/debito sono regolati e monitorati, in particolare per la Direzione Vendite e per il personale in trasferta.

La richiesta di emissione di carte di credito rientra tra i poteri dell'Amministratore Delegato/Direttore Generale e le carte sono assegnate alla Direzione Vendite.

È prevista la compilazione mensile di una nota spese e la presentazione dei giustificativi per gli acquisti effettuati con carta di credito. Il controllo delle note spese include la verifica degli importi con l'estratto conto mensile fornito dalla funzione Administration and Tax.

La gestione delle note spese e delle trasferte è coordinata dalla funzione Risorse Umane (RU) tramite il modulo ZTravel di Zucchetti, come riportato nella sezione 8.3.

Rapporti intercompany

Maticmind è la società madre del Gruppo Zenita (controllata da Mozart HoldCo S.p.A. e CDP Equity).

La Direzione Finance include un'area di Subsidiaries Finance Coordination per coordinare le attività finanziarie delle società controllate, allineandole agli obiettivi globali del gruppo.

Maticmind ha inoltre adottato un Regolamento di Gruppo per disciplinare i rapporti con le controllate, in particolare per le operazioni di carattere straordinario (come acquisizioni e modifiche rilevanti a budget e business plan) che richiedono l'autorizzazione preventiva del Consiglio di Amministrazione di Maticmind.

La funzione Group Marketing and Communication (centralizzata in Maticmind) si occupa invece di coordinare le attività di marketing e comunicazione di tutte le società del gruppo attraverso contratti di service intercompany, in base ai quali il costo del servizio erogato da Maticmind viene ribaltato sulle singole controllate, includendo un margine (sempre at arms length).

Rapporti con la Pubblica Amministrazione

Per quanto concerne i rapporti con la Pubblica Amministrazione, nell'ambito di eventuali interlocuzioni per l'ottenimento di garanzie e/o contributi pubblici, si veda la sezione 2.3.

Definizione del budget

Il processo di budgeting è centralizzato e segue un approccio dal basso verso l'alto (bottom-up).

La Direzione Finance (in particolare il Planning, Controlling & Reporting e la funzione Budgeting & Control) è responsabile del processo di pianificazione strategica dei ricavi e dei costi attesi.

La pianificazione è annuale (budget run) e parte dalle linee guida strategiche e dagli obiettivi definiti dall'Amministratore Delegato. I responsabili di funzione propongono i propri fabbisogni (OPEX) in fase di budget, che è poi soggetto a revisione e approvazione a più livelli, fino all'Amministratore Delegato.

Dopo l'approvazione del budget, l'acquisto di beni o servizi non è automatico. Ogni singola spesa significativa (come le spese rientranti nell'OPEX) deve essere autorizzata tramite una Richiesta di Acquisto (RdA) che segue un iter di approvazione gerarchica in base al valore economico della spesa, garantendo che il budget approvato non venga sforato. La Direzione Finance autorizza la spesa in base a soglie predefinite.

Il budget OPEX per la formazione e le iniziative di marketing è gestito dai responsabili di funzione.

1.4 Le procedure specifiche

L'area Finance e la gestione delle risorse finanziarie in Maticmind sono disciplinate da un insieme di procedure aziendali integrate nel Sistema di Gestione Integrato (SGI) a cui si fa integrale richiamo:

- Processo di Budgeting and Accounting Management (SGI_Linee Guida al Sistema di Gestione Integrato): definisce il processo di pianificazione strategica dei ricavi e dei costi (Budgeting), la sua approvazione da parte della Direzione Aziendale e la gestione e contabilizzazione dei costi;

- Microsoft Dynamics 365 (Manuale Operativo Navision): documentazione di riferimento relativa alle attività di gestione contabile, finanziaria e ERP della Società;
- Gestione Amministrativa Cliente (PAQ820_4): regolamenta le attività per la creazione dell'anagrafica cliente e l'apertura della linea di credito (fido), un prerequisito fondamentale per l'accettazione degli Ordini di Vendita e la gestione del rischio finanziario;
- Procedura di gestione dei regali, viaggi e sponsorizzazioni (PAQ820_4): stabilisce le regole e i limiti di spesa (max €150,00) per l'offerta o l'accettazione di regali, viaggi e sponsorizzazioni, per prevenire i reati di corruzione e garantire la trasparenza finanziaria.

2 SEZIONE 2: GOVERNANCE E GESTIONE DEGLI AFFARI LEGALI E SOCIALI

PROCESSI	ATTIVITÀ SENSIBILI	FUNZIONE COINVOLTA	REATI PRESUPPOSTO RILEVANTI
Gestione dei rapporti tra organi societari	- Convocazione assemblee, redazione verbali, nomina organi sociali	- CdA - General Counsel - Direzione Compliace, Sustainability, Risk Management & Safety - Marketing - Brand & Communication - Group Mergers & Acquisitions and Transformation - CFO - Consulente esterno	- Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24) - Delitti informatici e trattamento illecito (art. 24 bis) - Delitti di criminalità organizzata (art. 24 ter).e reati transnazionali (L. 146/2006) - Corruzione e traffico di influenze illecite (art. 25) - Reati societari (art. 25 ter) - Intermediazione illecita e sfruttamento del lavoro (art. 25 quinquies) - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio (art. 25 octies) - Reati in materia di violazione di misure restrittive dell'Unione Europea (art. 25 octies.2) - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci
Gestione dei contenziosi	- Gestione vertenze, arbitrati, negoziazione accordi transattivi		
Gestione dei rapporti contrattuali	- Gestione dei rapporti con i consulenti e collaboratori esterni - Negoziazione e sottoscrizione dei contratti		
Adempimenti societari	- Tenuta libri sociali, deposito bilanci, modifiche statutarie - Elaborazione e predisposizione del progetto di bilancio - Effettuazione delle riconciliazioni delle poste contabili - Elaborazione del budget e del business plan		
Gestione rapporti con enti pubblici	- Richieste di licenze, permessi, autorizzazioni - Partecipazione a bandi/finanziamenti - Gestione delle gare d'appalto e sottoscrizione dei relativi contratti - Accessi/Ispezioni/Verifiche da parte di pubblici ufficiali - Comunicazioni alle Autorità pubbliche di Vigilanza		

Gestione delle attività di marketing	- Omaggi e sponsorizzazioni		all'autorità giudiziaria (art. 25 decies) - Reati tributari (art. 25 quinquiesdecies)
Gestione delle operazioni straordinarie	- Decisioni strategiche in materia di M&A (individuazione delle target, scelte di riorganizzazione societaria tramite fusioni o altre operazioni straordinarie, etc.) - Svolgimento delle due diligence - Definizione delle condizioni contrattuali e negoziazione con controparte - Rapporti con la controparte, con i legali esterni e con i notai		

2.1 Alcuni esempi dei Reati Presupposto rilevanti nella Governance e Gestione Affari Legali e Sociali

Si riportano qui di seguito, a titolo esemplificativo, alcune delle potenziali condotte penalmente rilevanti in relazione alle Attività Sensibili sopra menzionate:

a) Corruzione e traffico di influenze illecite (art. 25)

- attraverso false stime degli investimenti, viene creata la provvista da offrire ad un funzionario pubblico o alla controparte privata in cambio di una condotta contraria ai doveri d'ufficio.

b) Reati societari (art. 25 ter)

- viene approvato un bilancio che contiene informazioni economico-patrimoniali false, gonfiando i ricavi e/o sottostimando i costi.

c) Reati tributari (art. 25 quinquiesdecies)

- vengono sottoscritti contratti di consulenza interamente o parzialmente fittizi a copertura di costi finalizzati a finanziare attività illecite o comunque non tracciate, con conseguente abbattimento dell'imponibile fiscale.

2.2 Le regole generali di condotta nella Governance e Gestione Affari Legali e Sociali

È fatto espresso divieto, a carico dei Destinatari, di:

- rappresentare o trasmettere dati falsi, lacunosi, parziali o comunque non rispondenti alla realtà sulla situazione economica, patrimoniale e finanziaria della Società, anche nei progetti di operazioni straordinarie, nonché nelle relazioni degli amministratori e degli esperti indipendenti;
- indicare false informazioni nelle certificazioni attestanti l'assenza o l'avvenuto soddisfacimento dei debiti verso le amministrazioni o gli enti pubblici;
- omettere dati e informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- alterare i dati e le informazioni destinati alla predisposizione del bilancio;
- illustrare i dati e le informazioni in modo tale da fornire una presentazione non corrispondente a quanto effettivamente maturato sulla situazione patrimoniale, economica e finanziaria dell'azienda e sull'evoluzione della sua attività;
- omettere informazioni rilevanti concernenti le società controllanti, controllate o collegate, ai sensi dell'art. 2359 c.c.;
- predisporre, stipulare, approvare o comunque porre in essere contratti o accordi formalmente redatti che risultino in tutto o in parte fittizi o privi di reale causa economica, ovvero operazioni inesistenti, simulate o con finalità fraudolente, finalizzate ad alterare la rappresentazione contabile, patrimoniale, fiscale o giuridica della Società o dei suoi rapporti con terzi;
- porre in essere, direttamente o indirettamente, atti di corruzione attiva o passiva, in qualsiasi forma o modo, nei confronti di pubblici ufficiali, incaricati di pubblico servizio o soggetti privati, italiani o stranieri e, in particolare, offrire, promettere, dare, ricevere o sollecitare denaro, utilità o altre forme di vantaggio non dovuto; esercitare pressioni o indebite influenze per ottenere o mantenere indebiti vantaggi nell'interesse o a vantaggio della Società; utilizzare intermediari, consulenti o soggetti terzi per finalità corruttive.
- stipulare contratti di appalto o fornitura di servizi che abbiano ad oggetto prestazioni lavorative prive di autonomia gestionale, organizzativa e di mezzi da parte del fornitore;
- omettere l'adozione o la verifica di specifici strumenti contrattuali e documentali finalizzati a garantire la tracciabilità, la liceità e la trasparenza del rapporto di appalto;
- violare le policy aziendali relative a omaggi, regalie e spese di rappresentanza, che devono sempre essere modiche, documentate e autorizzate;
- intraprendere qualsiasi iniziativa promozionale o di marketing finalizzata a ottenere indebiti vantaggi o ad influenzare decisioni di soggetti pubblici o privati.

2.3 I protocolli di condotta specifici

Nell'espletamento di tutte le operazioni attinenti all'Area di Rischio Governance e Gestione Affari Legali e Sociali, i Destinatari devono in ogni caso adottare e rispettare:

a. le norme del codice civile, nonché quelle applicabili in materia di contabilità, di tutela dell'integrità ed effettività del patrimonio sociale;

b. le procedure aziendali, la documentazione e le disposizioni inerenti alle strutture organizzativa gerarchico funzionale, al sistema amministrativo, contabile, finanziario e di controllo di gestione di Maticmind;

c. il Codice Etico.

In particolare, i Destinatari devono monitorare:

- i dati e le notizie che ciascuna funzione aziendale deve fornire stabilendo i criteri per la loro elaborazione e le tempistiche di trasmissione;
- la trasmissione dei dati e delle informazioni al CdA e al consulente esterno per via informatica, in modo che restino tracciati i vari passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- la tempestiva trasmissione al Collegio Sindacale della bozza di bilancio e della relazione della società di revisione o del soggetto incaricato del controllo contabile interno, nonché un'idonea registrazione di tale trasmissione;
- la previsione di riunioni tra la società di revisione ovvero il soggetto incaricato del controllo contabile interno, il collegio sindacale e l'Organismo di Vigilanza prima della approvazione del bilancio da parte del CdA e della sua sottoposizione all'Assemblea per la definitiva approvazione;
- la sottoscrizione da parte dei responsabili delle funzioni coinvolte nei processi di formazione della bozza di bilancio o di altre comunicazioni sociali di una dichiarazione di veridicità, completezza e coerenza dei dati e delle informazioni trasmessi;
- che ogni operazione e ogni transazione sia legittima, congrua, coerente, autorizzata e verificabile: a tale fine, tutte le transazioni devono essere correttamente e adeguatamente registrate e corredate di un supporto documentale completo, autentico e idoneo a consentire in ogni momento i controlli sulle caratteristiche e sulle motivazioni dell'operazione, nonché l'individuazione di chi ha autorizzato, effettuato, registrato e verificato l'operazione stessa;
- che la redazione del bilancio annuale e della relazione dell'organo amministrativo sulla gestione della Società, nonché tutte le altre rappresentazioni della situazione economico-finanziaria della Società, siano elaborati nel rispetto dei principi di veridicità, correttezza, completezza e accuratezza, segnalando tempestivamente le situazioni anomale e prestando particolare attenzione alla sussistenza di indicatori di crisi.

<u>Gestione delle operazioni sul capitale, utili e riserve</u>

La Società si attiene alle disposizioni di legge vigenti in materia ogni qualvolta pone in essere le seguenti operazioni, con specifico riferimento a capitale, utili e riserve:

- acquisto o vendita di azioni proprie;
- conferimento, trasformazione, riduzione del capitale sociale, fusione, scissione;
- distribuzione di riserve, utili, acconti su utili, anche in fase di liquidazione.

In ogni caso, la Società si impegna ad assicurare:

- precisa attribuzione delle responsabilità decisionali e di quelle operative nell'ambito dei singoli progetti, nonché i meccanismi di coordinamento tra le funzioni così individuate;
- al di fuori dei casi di legittima riduzione del capitale sociale, il preliminare controllo di legittimità del Collegio Sindacale, su ogni operazione di restituzione dei conferimenti ai soci, o di liberazione degli stessi dall'obbligo di eseguirli;
- in operazioni di distribuzione di utili o riserve di patrimonio netto, la preventiva verifica da parte di professionisti esterni della conformità alla normativa vigente;
- prima di attuare qualsiasi operazione sulle azioni, la verifica che perdite avvenute in corso di esercizio non abbiano eroso il patrimonio disponibile, rendendo impossibile l'operazione di acquisto o sottoscrizione, se non a costo di intaccare la consistenza del capitale o delle riserve indisponibili;
- per quanto riguarda l'eventuale conflitto di interessi, l'obbligo per il consigliere di comunicare all'Organismo di Vigilanza tutte le informazioni relative alle cariche assunte o alle partecipazioni di cui sia titolare, direttamente o indirettamente, in altre società o imprese, nonché le cessazioni o le modifiche delle medesime, le quali, per la natura o la tipologia, possono lasciar ragionevolmente prevedere l'insorgere di conflitti di interesse ai sensi dell'art. 2391 c.c.

<u>Gestione dei rapporti contrattuali</u>

Con riferimento ai contratti per la fornitura di beni e servizi si rimanda al paragrafo 5.3.

<u>Comunicazioni alle Autorità pubbliche di Vigilanza</u>

I Destinatari del Modello devono seguire le indicazioni e gli obblighi sottoelencati:

- la partecipazione a tutte le verifiche deve essere effettuata con la massima trasparenza ed integrità;
- l'obbligo di trasmettere alle Autorità i dati e i documenti specificamente richiesti dalle predette Autorità (e.g. bilanci e verbali delle riunioni degli organi societari);
- l'obbligo di collaborare nel corso di eventuali accertamenti ispettivi da parte delle funzioni competenti;
- la Società vieta espressamente qualsivoglia condotta volta ad alterare il giudizio dell'organo di controllo attraverso artifici, raggiri, o altri comportamenti finalizzati ad ottenere indebiti vantaggi;

- i Dipendenti, nell'ambito delle proprie competenze, sono tenuti a prestare all'Autorità di Vigilanza piena ed integrale collaborazione, onde consentire un corretto ed esaustivo svolgimento delle attività di verifica;
- la funzione appositamente incaricata è tenuta a predisporre un'apposita informativa sull'indagine avviata dall'Autorità, che dovrà essere periodicamente aggiornata in relazione agli sviluppi dell'indagine stessa ed al suo esito; tale informativa dovrà essere inviata all'OdV nonché agli altri uffici aziendali competenti in relazione alla materia trattata.

Rapporti con la P.A.

Maticmind intrattiene rapporti estesi con il settore pubblico e le istituzioni, principalmente attraverso una modalità di interazione indiretta o mediata, sebbene stia sviluppando anche rapporti diretti con enti concessionari.

La sua attività si svolge prevalentemente come fornitore nella catena di appalto e subappalto.

I rapporti con la Pubblica Amministrazione sono classificati in base al tipo di coinvolgimento:

- interazione tramite appalto (come subappaltatore): questi rapporti riguardano commesse che originano da gare d'appalto indette ai sensi della normativa sui contratti pubblici (D. Lgs. 50/2016), dove Maticmind agisce come subappaltatore per un operatore privato, che è l'aggiudicatario principale; i servizi forniti in regime di subappalto includono la fornitura di hardware e software, l'installazione e la manutenzione. In alcuni casi l'impegno può essere classificato come mera fornitura tecnologica se non prevede servizi complessi;
- rapporti con il Polo Strategico Nazionale (PSN): Maticmind intrattiene rapporti diretti o indiretti con il Polo Strategico Nazionale S.p.A., il quale opera come concessionario di servizio pubblico per la realizzazione e gestione di nuove infrastrutture informatiche per la PA, e non come stazione appaltante tradizionale, Con il PSN, Maticmind agisce come:
  - subfornitore di Vendor, per Vendor specifici che si siano aggiudicati una gara tecnologica indetta e gestita da PSN. In queste ipotesi, Maticmind ha rapporti contrattuali solo con il Vendor e non direttamente con PSN. Le prestazioni sono definite come subforniture in opera di beni, che possono includere attività accessorie come installazione e manutenzione, ma che non sono classificate come subappalto;
  - integratore di riferimento, qualora il Vendor vinca la gara e indichi Maticmind come integratore di riferimento, quest'ultima sottoscrive direttamente il contratto o l'accordo quadro con la committente PSN. Maticmind ha ad esempio sottoscritto direttamente con PSN accordi per la fornitura di server o servizi software;
- rapporti occasionali, per interlocuzioni amministrative, visite ispettive, contenziosi giudiziari.

Possono intrattenere rapporti con la Pubblica Amministrazione in nome e per conto di Maticmind esclusivamente i soggetti cui è stato formalmente conferito incarico o autorizzazione in tal senso, con apposita procura o disposizione organizzativa per i soggetti interni, ovvero con apposita clausola nel contratto di collaborazione, consulenza o partnership per i soggetti esterni. In particolare:

- Amministratore Delegato, che detiene altresì la rappresentanza legale;
- Procuratori Speciali per le rispettive aree di competenza.

Con particolare riferimento ai rapporti con esponenti della Pubblica Amministrazione:

- a tutti gli incontri con la P.A. e, in particolare, alle riunioni e gli incontri di particolare rilevanza, salvo i casi di motivata necessità o urgenza, partecipano almeno due rappresentanti della Società;
- a valle di ogni incontro deve essere redatto un verbale o, comunque, deve esservi traccia scritta (e-mail riepilogativa) di quanto avvenuto durante l'incontro;
- è assicurata, nel rispetto dei tempi e delle modalità stabiliti per le comunicazioni verso l'Organismo di Vigilanza, la tracciabilità dei rapporti formali con la Pubblica Amministrazione, intrattenuti dalle funzioni aziendali coinvolte;
- ove la Società si avvalga di un collaboratore o consulente esterno per essere rappresentata nei rapporti con la Pubblica Amministrazione, si applicano nei confronti del predetto collaboratore e consulente, nonché del relativo personale, le medesime direttive valide per i Destinatari e l'adozione di clausole contrattuali che impongono il rispetto dei principi del Codice Etico e del presente Modello, per quanto applicabile.

La Società assicura che:

- le attività connesse all'acquisizione di autorizzazioni, licenze, permessi, concessioni e provvedimenti simili della Pubblica Amministrazione siano condotte in maniera corretta, trasparente e tracciabile, nel rispetto della normativa applicabile;
- la documentazione e le informazioni necessarie per la richiesta di rilascio dei suddetti provvedimenti siano comunicate formalmente alla Pubblica Amministrazione dai soli soggetti formalmente delegati o autorizzati.

In particolare, la funzione interessata:

- nella predisposizione e produzione della documentazione necessaria secondo quanto previsto dalla normativa di riferimento e da specifiche disposizioni/richieste della Pubblica Amministrazione competente, acquisisce quanto richiesto, anche avvalendosi di operatori terzi o chiedendo, formalmente e per iscritto, alle funzioni competenti; i responsabili di dette funzioni sono tenuti a verificare e sottoscrivere tali dati, attestazioni e informazioni, sì da assicurarne la correttezza, veridicità e aggiornamento;
- garantisce/attesta il rispetto degli adempimenti connessi alla licenza/concessione/autorizzazione, anche sulla base di quanto documentato dalle funzioni competenti;
- provvede al monitoraggio, anche attraverso appositi scadenzari, della validità di ciascuna licenza/concessione/autorizzazione ottenuta, al fine di identificare la necessità di procedere al relativo rinnovo/proroga e di avviarne per tempo l'iter;

- è tenuta a garantire la tracciabilità dell'accoglimento o del rigetto dell'istanza da parte della Pubblica Amministrazione, nonché la conservazione di tutta la documentazione necessaria a consentire la verifica dell'espletamento degli adempimenti procedurali.

Con particolare riferimento alla gestione delle visite ispettive, i soggetti presenti per conto della Società sono tenuti a:

- coordinare e monitorare le attività di ispezione, anche delegando, se del caso, personale interno, in modo da soddisfare adeguatamente le esigenze manifestate dai pubblici ispettori;
- garantire che gli stessi siano accolti e dotati di tutti gli strumenti necessari per lo svolgimento delle attività di verifica;
- mettere a disposizione degli ispettori il personale necessario per l'efficiente espletamento delle attività ispettive;
- verificare e consegnare i documenti richiesti, sia contestualmente sia successivamente alla visita ispettiva, nel rispetto dei tempi e dei modi concordati con i pubblici ispettori;
- conoscere il luogo esatto in cui sono conservati gli atti, i documenti e le informazioni aziendali di competenza e l'eventuale soggetto terzo incaricato della conservazione e dell'archivio di tali atti, documenti e informazioni, anche al fine di fornire esatte indicazioni al riguardo agli enti di vigilanza e controllo che ne facciano richiesta; qualora non sia nelle condizioni di produrre quanto richiesto, attivarsi per acquisirlo, in modo formale e tracciato, dalle altre funzioni aziendali;
- tenere traccia dell'esito della verifica in un report interno, in cui indicare la natura della verifica ispettiva, le informazioni fornite, i rilievi effettuati e la posizione assunta dalla Società, allegando l'eventuale documentazione richiesta e consegnata;
- provvedere all'archiviazione delle copie dei verbali delle visite ispettive, dei relativi report interni e di tutta la documentazione prodotta o ricevuta nel corso delle predette visite.

È compito del personale incaricato, informare tempestivamente il proprio responsabile di ogni problematica che si dovesse ravvisare e di ogni relativa risposta, formale e informale, in merito alle richieste dei pubblici ispettori.

Gestione dei contenziosi

La Funzione Legal (General Counsel) è una delle principali responsabili della gestione degli aspetti legali che emergono nelle attività aziendali, offrendo pareri e supporto in caso di controversie e contenziosi legali, con il supporto di legali esterni a seconda della complessità del caso.

L'Amministratore Delegato/Direttore Generale detiene il potere di rappresentanza della Società in giudizio e di fronte a qualsiasi autorità. L'AD ha anche la facoltà di transigere e conciliare qualsiasi vertenza in sede giudiziale o stragiudiziale, fino a un limite di € 2.000.000 in firma singola.

Omaggi e liberalità

La Società ha definito regole chiare per l'offerta e l'accettazione di regali (omaggi e regalie) al fine di evitare potenziali conflitti di interesse.

A. Limiti per Destinatari Privati

Gli omaggi e le regalie verso controparti contrattuali private sono ammessi solo nei limiti dei normali rapporti di cortesia commerciale e non devono superare il valore di € 150,00. Altri protocolli di controllo confermano che omaggi e regalie ai privati sono ammessi entro un valore non superiore a € 100,00.

I regali concessi a terzi devono essere adeguatamente registrati nei libri contabili della Società.

B. Divieto verso Pubblici Ufficiali

È fatto assoluto divieto di disporre qualsiasi regalia (inclusi diarie o spese di piccola cassa) a funzionari della Pubblica Amministrazione o ai loro familiari.

Sponsorizzazioni

Le sponsorizzazioni rappresentano accordi con enti e società (di natura culturale, sportiva, etica, ecc.) attraverso i quali Maticmind (sponsor) fornisce supporto (finanziario o risorse) in cambio di un ritorno pubblicitario o altri benefici immateriali.

Le attività di sponsorizzazione sono gestite dalla funzione Brand & Communication a livello di Gruppo e il budget è sottoposto a un processo di budget run annuale e approvato dall'Amministratore Delegato

L'impiego del budget e le decisioni di sponsorizzazione si basano su criteri oggettivi e Key Performance Indicators (KPIs) predeterminati. I criteri includono:

- analisi dei dati storici (ritorno dell'evento, lead generate, affluenza);
- classificazione dell'evento (posizionamento, lead generation o legato a un partner vincolante da accordo di partnership);
- temi ESG (Environmental, Social, Governance), come progetti sociali o ambientali, che generano un ritorno di immagine.

Le sponsorizzazioni devono essere sottoposte al vaglio della Direzione Compliace, Sustainability, Risk Management & Safety per determinarne la "business justification".

Deve essere redatto un contratto dettagliato (oggetto, durata, corrispettivo, benefici attesi) e la spesa approvata seguendo le procedure aziendali. Il contratto deve essere firmato dall'Amministratore Delegato (indipendentemente dal suo valore) e deve includere l'accettazione del Modello e del Codice Etico da parte del soggetto sponsorizzato. Tutte le sponsorizzazioni sono registrate dal Marketing e comunicate alla Direzione Compliace, Sustainability, Risk Management & Safety.

La Direzione Compliace, Sustainability, Risk Management & Safety è responsabile del monitoraggio annuale e della verifica periodica dei registri relativi a regali, viaggi e sponsorizzazioni.

Verifiche e valutazione su partner e consulenti esterni

I professionisti esterni di cui si avvale la Società sono selezionati sulla base della loro iscrizione agli albi professionali di riferimento e dell'esperienza maturata nel settore. Sono inoltre soggetti a verifiche preliminari e periodiche in merito alla qualità dei servizi resi e all'aggiornamento normativo.

A seconda della strategicità e importanza del potenziale partner, vengono svolte due diligence preliminari per stabilirne l'affidabilità.

Si rinvia in ogni caso per la qualifica e le verifiche sui fornitori al paragrafo 5.3.

Rapporti con agenti e intermediari

Maticmind si avvale di soggetti terzi che possono agire come intermediari o procacciatori d'affari in diversi ambiti aziendali, in particolare per lo sviluppo del business e per le operazioni straordinarie.

In ogni caso, la Società riconosce e disciplina il ricorso a figure di intermediazione commerciale attraverso le sue deleghe di potere e procedure interne, sempre formalizzando i rapporti attraverso accordi scritti:

- poteri di nomina: l'Amministratore Delegato/Direttore Generale ha il potere di "nominare e revocare rappresentanti, depositari, agenti o commissionari";
- procacciatori d'affari: la Società può "concludere accordi con procacciatori d'affari e autorizzare e/o disporre il pagamento delle relative commissioni/corrispettivi". Tali operazioni sono soggette all'approvazione congiunta dell'Amministratore Delegato/Direttore Generale e di alcuni consiglieri, se l'importo della singola operazione supera i limiti di valore stabiliti;

Nelle operazioni di fusione e acquisizione, la funzione Group M&A and Transformation si avvale del supporto di soggetti esterni qualificati come advisor (consulenti) per il reperimento target: Le opportunità di acquisizione per Maticmind arrivano principalmente in due modi:

1. spontaneamente dalla rete di advisor (come banche d'investimento o boutique di M&A) che conoscono il Gruppo e i suoi azionisti;
2. in misura minore, tramite un accordo formalizzato con una specifica boutique di M&A per l'attività di scouting (ricerca preliminare), dietro remunerazione solitamente irrisoria.

Agli advisor esterni può venire riconosciuta una fee di intermediazione, nel solo caso in cui porta l'opportunità di acquisizione procacciata venga portata a termine. Tale compenso è definito ex ante tramite una lettera di ingaggio che stabilisce le attività svolte (come l'individuazione della target o supporto nella negoziazione) e la remunerazione (tipicamente una percentuale dell'enterprise value).

Rapporti intercompany

Con riferimento ai rapporti infragruppo, si rinvia al relativo paragrafo 1.3.

Operazioni straordinarie

La gestione delle operazioni straordinarie è affidata alla funzione Group Mergers & Acquisitions and Transformation, con il coinvolgimento dell'Amministratore Delegato, del Legal e del CFO.

Le attività relative a tale area seguono l'iter che segue:

i. individuazione: l'individuazione delle target avviene tramite advisor esterni o contatti interni. Se l'offerta preliminare è accettata, si avvia la due diligence che include, come minimo, verifiche legali, finanziarie e fiscali;
ii. valutazione rischi: in fase di due diligence, vengono analizzati anche i rischi di natura penale o fiscale, inclusa la presenza di un rischio rilevante ai sensi del Decreto o eventuali problemi degli amministratori che potrebbero ricoprire ruoli apicali post-acquisizione;
iii. decisione: la decisione di proseguire l'operazione, gestendo i rischi contrattualmente, o di interromperla, è presa di concerto dall'Amministratore Delegato, dal Legal e dal Finance (CFO). Se i rischi non possono essere mitigati da garanzie sufficienti, l'operazione viene interrotta;
iv. finanziamento: le acquisizioni sono finanziate tramite sia tramite debito che tramite capitale, la cui gestione è di competenza del CFO e dipende dalla disponibilità di cassa.

2.4 Le procedure specifiche

Al fine di prevenire o ridurre al minimo il rischio di commissione delle fattispecie di reato rilevanti nello svolgimento delle Attività Sensibili, la Società ha adottato delle procedure specifiche che costituiscono parte integrante del presente Modello e a cui si fa integralmente rinvio:

- Procedura di gestione dei regali, viaggi e sponsorizzazioni (PAQ820_4): stabilisce le regole e i limiti di spesa (max €150,00) per l'offerta o l'accettazione di regali, viaggi e sponsorizzazioni, per prevenire i reati di corruzione e garantire la trasparenza finanziaria.

3 SEZIONE 3: GESTIONE CONTABILE E ADEMPIMENTI FISCALI

PROCESSI	ATTIVITÀ SENSIBILI	FUNZIONE COINVOLTA	REATI PRESUPPOSTO RILEVANTI
Gestione della fatturazione attiva e passiva	- Gestione anagrafica clienti - Gestione anagrafica fornitori/consulenti - Emissione di fatture attive - Emissione di note di credito - Gestione del credito - Registrazioni di contabilità generale: contabilizzazione fatture, altre registrazioni di contabilità generale - Gestione delle richieste di pagamento dei fornitori/consulenti - Gestione delle fatture scadute - Emissione di note di debito	- Direzione Finance: - Administration & Tax - Finance & Treasury - Budgeting & Control - Subsidiaries Finance Coordination - Ufficio Amministrazione Banche - PGL - Direzione Commerciale	- Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24) - Delitti informatici e trattamento illecito dei dati (art. 24 bis) - Delitti di criminalità organizzata (art. 24 ter) e reati transnazionali (L. 146/2006) - Corruzione e traffico di influenze illecite (art. 25) - Reati societari (art. 25 ter) - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio (art. 25 octies) - Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (Art. 25 octies 1) - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 duodecies) - Reati tributari (art. 25 quinquiesdecies)
Gestione amministrativa del personale	- Rilevazione di presenze, straordinari, permessi e ferie del personale dipendente - Elaborazione degli stipendi e/o compensi e tutte le spettanze da liquidare ai dipendenti - Calcolo dei contributi e delle trattenute fiscali inerenti ai corrispettivi - Comunicazioni ed invio alle competenti Autorità Pubbliche delle dichiarazioni contributive e versamento dei		

	contributi previdenziali, assistenziali e fiscali - Gestione note spese e spese di rappresentanza		
Gestione degli adempimenti fiscali	- Gestione degli adempimenti e dei rapporti con le Autorità Pubbliche (es. in ambito amministrativo, previdenziale, assistenziale e tributario) - Elaborazione telematica del modello F24 e versamento delle ritenute - Elaborazione delle certificazioni delle ritenute operate a titolo di sostituto d'imposta - Predisposizione della dichiarazione e versamento IVA - Elaborazione scadenziario - Elaborazione del Modello Unico e versamento dell'IRES/IRAP - Elaborazione del 770 e qualunque altra reportistica fiscale - Predisposizione della documentazione rilevante in materia di prezzi di trasferimento - Versamento delle imposte - Gestione degli adempimenti fiscali riguardanti le operazioni di import/export intracomunitarie ed extracomunitarie		

3.1 Alcuni esempi dei Reati Presupposto rilevanti nella Gestione contabile e adempimenti fiscali

Si riportano qui di seguito, a titolo esemplificativo, alcune delle potenziali condotte penalmente rilevanti che potrebbero verificarsi in relazione alle Attività Sensibili sopra menzionate:

a) Reati societari (art. 25 ter)

- vengono inseriti in bilancio valori superiori a quelli reali alla voce "rimanenze di magazzino", al fine di mostrare una situazione patrimoniale più solida e facilitare così l'accesso a crediti bancari o finanziamenti a condizioni più favorevoli.

b) Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25 octies)

- le somme provento di reati tributari (indebita detrazione IVA) vengono investite in operazioni di investimento e/o finanza strutturata.

c) Reati tributari (art. 25 quinquiesdecies)

- contabilizzazione di fatture per operazioni oggettivamente o soggettivamente inesistenti, con conseguente indebito risparmio delle imposte sui redditi e/o dell'IVA.

3.2 Regole generali di condotta nella Gestione contabile e adempimenti fiscali

I Destinatari della presente Parte Speciale devono:

- rispettare la normativa vigente in materia contabile, tributaria e fiscale, nazionale e internazionale, nonché le procedure interne aziendali applicabili;
- registrare ogni operazione contabile in modo veritiero, accurato, completo e tempestivo, assicurando la corretta rappresentazione della situazione economica, patrimoniale e finanziaria della Società;
- garantire la tracciabilità e la documentazione di ogni operazione economica o finanziaria, in modo da consentire la verifica del processo decisionale, autorizzativo e attuativo;
- evitare qualsiasi comportamento volto a occultare o alterare documenti contabili, fiscali o tributari, o a impedire o ostacolare le attività di controllo interno o di revisione legale;
- non predisporre o utilizzare documentazione contabile o fiscale falsa, incompleta o ingannevole, anche al fine di ottenere indebitamente benefici fiscali, contributivi o finanziamenti pubblici;
- collaborare pienamente con le autorità fiscali e di controllo, fornendo dati e informazioni veritieri e trasparenti, anche in sede di verifiche, ispezioni o accertamenti;
- astenersi dal porre in essere operazioni simulate o artificiose che possano determinare l'emissione o l'utilizzo di fatture per operazioni inesistenti o la rappresentazione falsa nelle scritture contabili;

- verificare l'identità, l'affidabilità e la legittimazione dei soggetti con cui la Società intrattiene rapporti economici e commerciali, assicurandosi che non presentino profili di rischio connessi al riciclaggio o all'impiego di proventi illeciti;
- evitare l'accettazione o l'effettuazione di pagamenti in contanti o attraverso strumenti non tracciabili, privilegiando modalità di pagamento trasparenti e completamente riconducibili ai soggetti coinvolti;
- rifiutare operazioni che presentino elementi anomali o incoerenti rispetto alla natura del rapporto commerciale (importi sproporzionati, richieste di pagamenti frazionati, utilizzo di intermediari non giustificati, ecc.);
- verificare la provenienza lecita di beni, servizi o fondi impiegati in operazioni aziendali, evitando di acquistare beni o ricevere fondi di cui non sia possibile accertare la provenienza o il legittimo possessore;
- astenersi da qualsiasi comportamento che possa agevolare, anche indirettamente, l'introduzione nel circuito economico-finanziario di proventi derivanti da attività illecite;
- evitare qualsiasi forma di elusione o frode fiscale, anche mediante l'interposizione fittizia di soggetti terzi o l'utilizzo di strutture societarie non giustificate da valide ragioni economiche;
- attuare controlli e riconciliazioni contabili periodiche, garantendo l'integrità e la coerenza dei dati rispetto ai documenti giustificativi e agli obblighi fiscali connessi.

Nella gestione degli adempimenti fiscali, Maticmind assicura inoltre che le attività inerenti siano condotte in maniera corretta, trasparente e tracciabile, nel rispetto della normativa applicabile alla Società e che sia attuata un'adeguata gestione del rischio fiscale, garantendo:

- il corretto trattamento fiscale delle componenti di reddito, secondo quanto previsto dalla normativa di riferimento, e il corretto e puntuale assolvimento degli obblighi normativi in materia di predisposizione delle dichiarazioni fiscali periodiche relative alle imposte sui redditi e sul valore aggiunto, in materia (inter alia) di detrazioni, deduzioni e compensazioni, nonché il puntuale pagamento di tutte le imposte;
- l'analisi e l'interpretazione della normativa fiscale/doganale applicabile alla Società;
- la diffusione delle principali novità normative in materia fiscale/doganale nonché il supporto al personale coinvolto nella gestione degli aspetti fiscali, anche al fine di valutare gli impatti della normativa fiscale sulle attività di business;
- l'accuratezza e la completezza dei documenti e delle informazioni amministrativo-contabili utilizzati per il calcolo delle imposte, oggetto di comunicazione/trasmissione tramite sistemi informatici a studi legali/tributari esterni per le attività di competenza;
- il monitoraggio costante, anche attraverso uno scadenziario, degli adempimenti di legge, al fine di evitare ritardi e imprecisioni nella presentazione delle dichiarazioni e/o documenti fiscali/doganali;
- la corretta predisposizione delle dichiarazioni obbligatorie di legge/i modelli di pagamento sulla base delle disposizioni normative vigenti;

- la conservazione e l'archiviazione, secondo modalità atte a garantirne la riservatezza e la protezione da accessi non autorizzati, della documentazione amministrativo-contabile inerente alla gestione degli aspetti fiscali;
- la tempestiva comunicazione al CdA di eventuali problematiche e/o anomalie riscontrate, per la definizione delle azioni da intraprendere;
- correttezza, trasparenza e tracciabilità nella gestione dei rapporti con gli Enti di Controllo in materia fiscale (Guardia di Finanza, Agenzia delle Entrate, Agenzia delle Dogane, etc.), con riferimento, in particolare, all'analisi e alla verifica circa la corretta gestione degli adempimenti in materia da parte della Società.

3.3 I protocolli di condotta specifici

L'Accounting Management è presidiato principalmente dalla Direzione Finance e dalla funzione Administration & Tax, integrando strettamente i sistemi informativi aziendali e i protocolli di controllo per garantire la conformità e la trasparenza. La Direzione Finance, sotto la supervisione del CFO, è suddivisa in diverse funzioni che cooperano nella gestione contabile e fiscale:

Administration & Tax: questa funzione gestisce i processi fondamentali di registrazione contabile, inclusi:

- fatturazione attiva e fatturazione passiva;
- ricezione merce e ricezione servizio (entrata merce/servizio);
- acquisto e contabilizzazione dei cespiti e delle relative movimentazioni;
- contabilizzazione delle imposte civilistiche correnti e differite.

Ufficio Amministrazione Banche: sebbene sia focalizzato sulla tesoreria, partecipa alla gestione contabile attraverso la registrazione della prima note banche e la riconciliazione dei saldi bancari.

Planning, Controlling & Reporting (Controllo di Gestione): non gestisce direttamente la contabilità operativa, ma utilizza i dati contabili per il reporting gestionale, inclusa l'elaborazione di report come il managing (mensile), il bilancio (trimestrale) e i forecast, destinati alla Direzione aziendale e agli azionisti.

Il processo contabile è supportato dai sistemi informativi aziendali (SIA), al fine di assicurare la tracciabilità:

- ERP Finanziario (Navision/Microsoft Dynamics 365): il sistema gestionale Navision (ora Microsoft Dynamics 365 Business Central) è l'ERP aziendale di riferimento, utilizzato per la contabilità generale e analitica;
- SIM/Presales: questo sistema informativo è il motore del workflow commerciale. Registra le evidenze prodotte durante le attività, inclusa la scheda di lavoro (SDL), e supporta la Direzione Amministrazione nel controllo dei flussi informativi che vengono poi trasposti nei libri contabili e nel bilancio.

Gestione della contabilità e dei cicli attivo e passivo

A. Ciclo passivo (acquisti e pagamenti)

Il ciclo passivo in Maticmind è un macro-processo strutturato volto a garantire che l'approvvigionamento di beni e servizi avvenga in modo controllato, tracciabile e conforme alle normative (in particolare al D. Lgs. 231/2001). La gestione è centralizzata presso la Direzione Finance e la Direzione Acquisti, con il supporto operativo delle Business Unit e della Logistica.

Le fatture vengono scaricate dallo SDI (per i fornitori italiani) o ricevute via email/portale (per i fornitori esteri). Il processo di contabilizzazione dell'ufficio ACF include:

- verifica della coerenza tra fattura, OdA ed EM/ES (prezzi, quantità, IBAN);
- la fattura viene abbinata elettronicamente all'Entrata Merce o Servizio su NAVision;
- per i fornitori UE/Extra-UE, viene predisposto il Modello Intrastat e generato un file XML per lo SDI per comprovare la ricezione.

Le fatture per servizi di consulenza seguono controlli specifici sulla natura del contratto e su eventuali compensi variabili, con l'applicazione delle ritenute d'acconto.

Il ciclo si conclude con il pagamento, gestito dall'Ufficio Amministrazione Banche:

- mensilmente viene estratto lo Scadenzario Fornitori da NAVision per analizzare le fatture in scadenza;
- le distinte di pagamento richiedono una firma autografa della Direzione Amministrativa e una successiva approvazione digitale tramite token da parte di soggetti con poteri di firma (AD o Procuratori);
- il pagamento avviene solitamente tramite bonifico, finanziamenti commerciali o Fin.import per acquisti esteri.

Con riferimento ai profili relativi al processo di approvvigionamento, si rinvia al paragrafo 6.3.

B. Ciclo attivo

Il ciclo attivo copre l'intera catena del valore, dall'individuazione dell'opportunità commerciale fino all'incasso del credito, ed è finalizzato a garantire efficacia operativa e conformità normativa.

Il processo è governato principalmente dalle Direzioni Commerciale, Operations e Finance e si articola nelle seguenti fasi principali:

i. Pre-vendita e progettazione dell'offerta

Il ciclo inizia con l'individuazione di un'esigenza del Cliente e la creazione di un'anagrafica nel sistema SIM/Presales.

- Processo Go/No-Go: le opportunità sono sottoposte a una valutazione preventiva (soprattutto per gare e offerte complesse) che coinvolge le funzioni tecnica, finance, legal e HR per analizzare rischi, marginalità e requisiti di compliance.

- Solution engineering: la struttura di prevendita elabora la soluzione tecnica e il piano costi/ricavi (tramite il Compositore di Offerta - CDO).
- Verifica del credito: l'Ufficio Amministrazione Contabilità Clienti (ACC) effettua un'analisi di affidabilità per la concessione del fido, requisito indispensabile per procedere con l'ordine.

ii. Gestione dell'Ordine di Vendita (OdV)

Una volta ricevuto l'ordine formale dal Cliente, la Segreteria Commerciale (SC) e il Key Account Manager (KAM) procedono come segue:

- Riesame: il KAM verifica la coerenza tra l'ordine ricevuto e l'offerta approvata.
- Registrazione: la SC crea l'Ordine di Vendita nel sistema SIM, associandolo univocamente alla Scheda di Lavoro (SDL).
- Approvazione: l'OdV segue un iter autorizzativo basato su soglie di spesa e marginalità, che può richiedere la firma dell'Amministratore Delegato per importi elevati.

iii. Esecuzione (Delivery) e Service Management

L'approvazione dell'ordine attiva la Direzione Operations, che assegna un Project Manager (PM) per l'installazione o un Service Manager (SM) per l'assistenza.

- Esecuzione: include l'approvvigionamento dei materiali tramite l'Ufficio Acquisti e le attività tecniche di configurazione e test sul campo.
- Benestare (BEF): al termine dei lavori, il PM o la funzione PGL richiede al Cliente il Benestare all'Emissione della Fattura (BEF) o la firma del Modulo Intervento Tecnico (MIT), necessari per sbloccare la fatturazione.

iv. Fatturazione Attiva

L'Ufficio Amministrazione Contabilità Clienti (ACC) gestisce l'emissione dei documenti fiscali tramite il sistema ERP NAVision.

- Emissione: viene generata una fattura elettronica in formato .xml, trasmessa tramite il portale ARXivar al Sistema di Interscambio (SDI) dell'Agenzia delle Entrate.
- Controlli: prima dell'invio, l'ufficio verifica la corrispondenza degli importi con il BEF e l'ordine originario, oltre al rispetto dei termini di pagamento.

v. Tesoreria e Credit Management

L'ultima fase riguarda la riscossione del credito e la gestione finanziaria degli incassi.

- Rilevazione incassi: l'Ufficio Amministrazione Banche monitora giornalmente i movimenti tramite l'Home Banking e invia i dati all'ufficio ACC per la contabilizzazione.
- Gestione del credito: Viene effettuato un monitoraggio costante dell'ageing dei crediti; in caso di ritardi, vengono attivati solleciti o, se necessario, procedure legali di recupero previa valutazione della Direzione Amministrativa.
- Strumenti finanziari: per Clienti specifici come Fastweb e Telecom, Maticmind utilizza soluzioni di Factoring (pro-soluto) o Reverse Factoring per ottimizzare i flussi di cassa.

Gestione degli adempimenti fiscali

La gestione degli adempimenti fiscali è centralizzata all'interno della Direzione Finance, sotto la supervisione del Chief Financial Officer (CFO), e si avvale della collaborazione di consulenti fiscali esterni per la predisposizione e l'invio delle dichiarazioni.

Le attività operative sono suddivise tra diverse unità amministrative per garantire la segregazione dei compiti:

- Administration & Tax (Amministrazione & Fiscale): gestisce i processi di fatturazione attiva e passiva, la contabilizzazione dei cespiti e monitora i crediti tributari e i contenziosi fiscali.
- Ufficio Amministrazione Banche: è responsabile dei rapporti con gli istituti di credito, dello scarico giornaliero dei movimenti bancari e della contabilizzazione delle imposte civilistiche correnti e differite.
- Ufficio Amministrazione Contabilità Fornitori: si occupa del calcolo della liquidazione IVA tramite il sistema ERP NAVision e della creazione dei file di supporto per rilevare i saldi mensili.
- Payroll Specialist (HR): supervisiona gli adempimenti periodici (F24, flussi Uniemens) e annuali (modelli CU e 770, autoliquidazione INAIL) relativi al personale.

i. Gestione dell'IVA

Il processo segue una scansione temporale rigorosa supportata da flussi informatici:

1. Liquidazione mensile: dopo le chiusure contabili, l'Ufficio Amministrazione Fornitori lancia il calcolo dell'IVA su NAVision e predispone un file Excel con i dati a credito e a debito del mese.
2. Li.Pe. (liquidazioni periodiche): entro il secondo mese successivo al trimestre di competenza, i dati vengono inviati al consulente esterno, che provvede alla trasmissione telematica all'Agenzia delle Entrate.
3. Dichiarazione annuale: nel mese di aprile dell'anno successivo, l'Ufficio Amministrazione Banche trasmette al consulente il dettaglio della situazione IVA annuale; la bozza prodotta dal consulente deve essere verificata e approvata formalmente da Maticmind prima dell'invio definitivo.

ii. Imposte sul reddito e consolidato fiscale

A partire dall'esercizio 2023, Maticmind ha optato per il regime del consolidato fiscale nazionale come società controllante (insieme a Cloudmind S.p.A. e Fibermind S.r.l.), il che permette di determinare l'IRES su una base imponibile unica.

- Calcolo delle imposte: il responsabile dell'Ufficio Amministrazione Banche invia la bozza di bilancio al consulente esterno, che calcola le imposte provvisorie.
- Verifica e contabilizzazione: dopo un controllo interno sulla correttezza dei calcoli (con eventuale richiesta di modifiche), l'ufficio procede alla contabilizzazione delle imposte definitive su NAVision.
- Fiscalità differita: le imposte anticipate e differite vengono iscritte in bilancio sulla base delle differenze temporanee tra valori civilistici e fiscali, seguendo il principio della prudenza riguardo alla ragionevole certezza del loro recupero futuro.

iii. Altri adempimenti e tracciabilità

Con riferimento alla certificazione dei compensi a terzi, l'Ufficio Amministrazione Fornitori compila annualmente la certificazione del versamento delle ritenute d'acconto effettuate a favore di consulenti e professionisti.

Con riferimento al Modello Intrastat, per le operazioni intracomunitarie, l'Ufficio Amministrazione Contabilità Fornitori predispone i dati relativi alla nomenclatura delle merci e dei servizi, inviandoli al consulente per la trasmissione entro il 25 del mese successivo.

<u>Gestione delle spese di rappresentanza</u>

In linea con la circolare Assonime 26/2025, per garantire l'esenzione fiscale dei rimborsi ai dipendenti e la deducibilità delle spese per la Società, tutte le spese di trasferta e rappresentanza sostenute in Italia devono essere pagate con strumenti tracciabili (carte, bonifici, assegni, app collegate a conti). Sono pertanto vietati i pagamenti in contanti per tali categorie di spesa, con uso preferenziale di carte o conti aziendali. Restano esclusi dall'obbligo i trasporti pubblici di linea e le spese sostenute all'estero.

La Società assicura dunque che:

- ogni pagamento e rimborso sia documentato da ricevuta/fattura e prova della tracciabilità;
- siano compilate e verificate formalmente le note spese;
- sia conservata la documentazione sottostante alle richieste di rimborso;
- siano svolti controlli periodici su tali adempimenti
- siano periodicamente impartite formazione e istruzioni operative ai dipendenti, al fine di garantire uniformità e prevenire indeducibilità o imponibilità in caso di irregolarità.

Con riferimento agli ulteriori aspetti relativi alla gestione amministrativa del personale si rinvia al paragrafo 8.3.

3.4 Le procedure specifiche

Al fine di prevenire o ridurre al minimo il rischio di commissione delle fattispecie di reato rilevanti nello svolgimento delle Attività Sensibili, la Società ha adottato delle procedure specifiche che costituiscono parte integrante del presente Modello e a cui si fa integralmente rinvio:

- SGI_Processo di Budgeting and Accounting Management, che regola il processo di pianificazione strategica dei ricavi e dei costi (budgeting) e la successiva gestione e contabilizzazione dei costi e dei servizi;
- MM_PAM002_Fatturazione Attiva, che descrive le attività svolte per gestire il processo di fatturazione attiva specificando le funzioni aziendali coinvolte e le responsabilità operative di ciascuna delle funzioni e le relative applicazioni del sistema informativo aziendale;
- MM_PAMM003_Fatturazione Passiva, che descrive le attività svolte per gestire il processo di fatturazione passiva specificando le funzioni aziendali coinvolte e le responsabilità operative di ciascuna delle funzioni e le relative applicazioni del sistema informativo aziendale;
- MM_PAMM006_Tesoreria e Fiscalità descrive le attività svolte dalla Direzione Amministrativa per gestire il ciclo degli incassi, dei pagamenti e degli adempimenti fiscali.

4 SEZIONE 4: SALES

AREA A RISCHIO	ATTIVITÀ SENSIBILI	FUNZIONE COINVOLTA	REATI PRESUPPOSTO RILEVANTI
Gestione dei rapporti con il cliente	- Acquisizione del cliente e business. develpment - Trattative con enti pubblici o aziende a partecipazione pubblica o clienti privati - Omaggi - Gestione dei reclami	- Direzione Commerciale - Segreteria Commerciale (SC) - Funzioni di Prevendita - Key Account Manager (KAM) - Sales Executive (SE) - Architects - Amministratore Delegato - CISO - Legal - Direzione Compliace, Sustainability, Risk Management & Safety - HR - Operations - Finance - Direzione Amministrativa (Ufficio clienti)	- Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24) - Delitti informatici e trattamento illecito (art. 24 bis) - Delitti di criminalità organizzata (art. 24 ter) e reati transnazionali (L. 146/2006) - Corruzione e traffico di influenze illecite (art. 25) - Reati societari (art. 25 ter) - Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio (art. 25 octies) - Reati in materia di violazione di misure restrittive dell'Unione europea (art. 25 octies.2)
Gestione dei rapporti con agenti e intermediari	- Selezione degli agenti e degli intermediari e relativi rapporti		
Gestione degli ordini e delle negoziazioni contrattuali	- Gestione delle piattaforme per la partecipazione alle gare - Predisposizione della documentazione - Contrattazione dei termini e delle condizioni contrattuali - Definizione del prezzo - Definizione del budget e dei costi		
Pianificazione operativa e progettazione della commessa/ordine	- Progettazione dell'impianto - Definizione della componentistica e delle materie prime necessarie		

4.1 Alcuni esempi dei Reati Presupposto rilevanti nell'Area Sales

Si riportano qui di seguito, a titolo esemplificativo, alcune delle potenziali condotte penalmente rilevanti che potrebbero verificarsi in relazione alle Attività Sensibili sopra menzionate:

a) Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione europea per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24)

   - durante la partecipazione ad una gara di appalto pubblica, avvengono interlocuzioni illecite con i membri della commissione aggiudicante che permettono alla Società di ottenere informazioni indispensabili per vincere la gara.

b) Corruzione e traffico di influenze illecite (art. 25)

   - viene pagata a un agente una somma non dovuta, che costituisce la provvista per corrompere un pubblico ufficiale e ottenere l'aggiudicazione di una gara d'appalto.

c) Reati societari (art. 25 ter)

   - vengono promesse utilità al legale rappresentante di una società privata perché affidi alla Società un importante contratto di appalto.

4.2 Le regole generali di condotta nell'Area Sales

I Destinatari della presente Parte Speciale devono:

- astenersi dall'offrire, promettere o concedere omaggi, regalie o altri vantaggi non simbolici a Clienti, pubblici ufficiali o soggetti collegati a enti pubblici o partecipati;
- condurre ogni trattativa con enti pubblici, aziende partecipate o clienti privati in modo trasparente, tracciabile e documentato;
- rispettare rigorosamente le normative anticorruzione, nazionali e internazionali;
- evitare ogni alterazione di documenti o sistemi informatici;
- assicurarsi che la selezione di agenti e intermediari avvenga sulla base di criteri trasparenti, oggettivi e verificabili e che i relativi compensi siano stabiliti in maniera altrettanto trasparente e verificabile tramite contratti scritti, evitando di riconoscere provvigioni non dovute e/o non adeguatamente giustificate;
- effettuare, in fase di selezione di agenti e intermediari, una verifica reputazionale e di idoneità tecnico-operativa a svolgere l'attività richiesta;
- formalizzare ogni rapporto contrattuale, garantendo che i termini e le garanzie siano definiti in modo chiaro e tutelino gli interessi aziendali nel rispetto delle normative e includendo clausole di conformità al Modello e al Codice Etico, a pena di risoluzione del contratto;
- utilizzare esclusivamente credenziali personali e autorizzate per accedere a piattaforme di gara;

- redigere e presentare documentazione veritiera, completa e coerente, evitando qualsiasi falsa dichiarazione;
- tracciare e documentare tutte le comunicazioni con il Cliente o con l'ente appaltante;
- garantire che ogni interlocuzione sia condotta nel rispetto delle regole di correttezza e legalità;
- effettuare la selezione di partner terzi secondo procedure aziendali trasparenti e conformi alla normativa vigente;
- redigere budget e piani economici basati su criteri di veridicità, congruità e coerenza con gli obiettivi aziendali, evitando qualunque forma di alterazione dei costi e dei dati inseriti;
- condurre le negoziazioni e interlocuzioni nel rispetto dei principi di correttezza, legalità e buona fede, documentando tutte le fasi del processo;
- nello sviluppo dei progetti con Clienti/committenti, rispettare la normativa in materia di proprietà intellettuale e industriale, prestando particolare attenzione alla titolarità dei diritti di sfruttamento economico su opere dell'ingegno, marchi, brevetti, segni distintivi, disegni o modelli;
- adottare comportamenti improntati alla diligenza, correttezza, trasparenza e responsabilità nell'accesso, nella gestione e nella conservazione delle informazioni, in particolare quelle contenenti dati personali, riservati, strategici o coperti da segreto industriale.

È inoltre fatto divieto di:

- vendere o fornire servizi a soggetti sanzionati o riconducibili a Paesi sotto embargo, o comunque fornire servizi remoti o accesso a software a clienti non autorizzati;
- alterare o falsificare documenti di vendita o spedizione, valori o classificazioni, o comunque aggirare licenze attraverso triangolazioni, intermediari fittizi o consegne frazionate.

4.3 I protocolli di condotta specifici

La gestione del processo di vendita (Sales) in Maticmind è un'attività complessa e strutturata che si sviluppa attraverso diverse fasi, dalla generazione dell'opportunità fino all'esecuzione del servizio e alla fatturazione, ed è strettamente regolamentata da procedure interne (PAQ) e sistemi informativi per garantirne la tracciabilità e la conformità.

Il processo è guidato principalmente dalla Direzione Commerciale e dalla Segreteria Commerciale (SC), con il supporto delle funzioni di Prevendita, Operations e Finance.

1. Struttura della Direzione Commerciale

La Direzione si articola su quattro Industries principali: Mercato Pubblico (diviso in PA Centrale e PA Locale), Telco & Utilities, Finanza e Assicurazioni, e Large Account e SME.

- Ruoli chiave: il Key Account Manager (KAM) o Sales Executive (SE) è il titolare del rapporto con il Cliente, responsabile dell'identificazione delle opportunità commerciali e del coordinamento della proposta.
- Supporto alla vendita: i team di Prevendita (Solution Engineering) e gli Architects (specialisti tecnici) supportano il KAM nella progettazione e nell'elaborazione delle offerte, specialmente quelle complesse o per i bandi di gara.

2. Fasi del Processo di Vendita

A. Pre-vendita e progettazione dell'Offerta

1. individuazione dell'esigenza e registrazione: il KAM raccoglie i requisiti del Cliente e formalizza l'opportunità creando una Scheda di Lavoro (SDL) nel Sistema Informativo Aziendale (SIM/Presales), che funge da contenitore per tutta la documentazione e i flussi di lavoro;
2. valutazione dell'opportunità (processo Go/Not-Go): per le opportunità della Direzione Vendite Area Mercato (Public Sector, Finance, etc.), è obbligatorio seguire il processo Go Not Go, ideato per la valutazione preventiva di opportunità che presentano rischi elevati, complessità, margini bassi, o l'uso di subappalti non qualificati. Il processo è supervisionato dal Comitato Decisionale, che include figure apicali (Amministratore Delegato, CFO, CISO) e funzioni di supporto (Legal, Compliance, HR), per valutare i rischi di compliance, finanziari e tecnici.

   La valutazione dell'opportunità include le verifiche KYC e di due diligence preventiva, volte a mitigare i rischi legati al riciclaggio e alla non conformità. I principali requisiti e controlli di due diligence sui Clienti includono:

   - analisi amministrativa e finanziaria: l'Ufficio Clienti (all'interno della Direzione Amministrazione) è responsabile di analizzare la visura societaria e i bilanci della controparte contrattuale per gli ultimi tre esercizi commerciali, con lo scopo di evidenziare eventuali anomalie contabili;
   - verifica di affidabilità: deve essere verificata l'attendibilità commerciale e professionale delle controparti alla luce degli indicatori di anomalia emanati dall'UIF (Unità di Informazione Finanziaria). Tali indicatori possono riguardare, ad esempio, se l'impresa è di recente costituzione, se ha un oggetto sociale particolarmente ampio, o se i soci o amministratori hanno un dubbio profilo reputazionale (per precedenti penali connessi a reati patrimoniali, fiscali o fallimentari, o se risultano nullatenenti o irreperibili);
   - rapporti con Paesi ad alto rischio: per operazioni che coinvolgono Paesi terzi ad alto rischio, l'Ufficio Clienti deve richiedere informazioni aggiuntive riguardo lo scopo e la natura del rapporto, l'origine dei fondi, e la situazione economico-patrimoniale del Cliente;
   - gestione del fido: la concessione del fido ai Clienti è gestita esclusivamente tramite strumenti informatici per garantirne la massima tracciabilità e trasparenza.

3. Elaborazione tecnica e commerciale: la funzione Prevendita elabora la soluzione tecnica e definisce i costi/ricavi attraverso l'applicazione Compositore di Offerta (CDO), che confluisce nell'Offerta di Vendita;
4. verifica del credito (fido): per i nuovi Clienti, la Direzione Amministrazione verifica la linea di credito (fido) e l'affidabilità finanziaria del Cliente. La concessione del fido è un requisito indispensabile per accettare Ordini di Vendita e garantisce la tracciabilità e la trasparenza;
5. approvazione dell'Offerta: l'Offerta è soggetta a limiti di firma basati sul valore economico e sulla marginalità prevista, con approvazione a più livelli che può estendersi all'Amministratore Delegato per gli importi superiori.

B. Gestione dell'Ordine di Vendita

1. Ricevimento e riesame: la Segreteria Commerciale (SC) prende in carico l'Ordine Cliente (ricevuto via PEC o portale) e lo smista al KAM/SE. Il KAM riesamina l'ordine per verificarne la coerenza con l'Offerta approvata, specialmente in caso di modifiche di quantità o condizioni;
2. generazione OdV: in caso di esito positivo, la SC registra l'Ordine di Vendita (OdV) nel sistema SIM/Presales. Se il fido del Cliente non è attivo o capiente, il sistema blocca il processo;
3. autorizzazione OdV: l'OdV è approvato dal KAM/SAM secondo le deleghe di spesa. Tale approvazione è un vincolo per l'attivazione della fase successiva;
4. emissione Ordine di Acquisto (OdA): l'approvazione dell'OdV (per i prodotti) o l'emissione di una Richiesta di Acquisto (RdA) (per i servizi) da parte della Direzione Operation autorizza la funzione Acquisti (Procurement) a emettere i relativi Ordini di Acquisto verso i fornitori.

Controlli di trade compliance

Maticmind svolge controlli specifici, nonché di raccolta e verifica informazioni in ambito trade compliance, secondo l'iter che segue. Al termine dei controlli descritti sotto, è rimessa alla funzione compliance, con l'eventuale supporto di legali o doganalisti esterni, ogni valutazione quanto alla necessità di ottenere autorizzazioni o licenze per la vendita.

I controlli si focalizzano sia sui prodotti dual use, che sui prodotti e i servizi potenzialmente oggetto di misure restrittive unionali, e prevedono:

- la classificazione dei prodotti venduti;
- la raccolta di informazioni sul Paese di destinazione, end-use ed end-user;
- la conservazione della documentazione rilevante;
- la gestione degli aspetti doganali relativi alle dichiarazioni per poter spedire prodotti in conformità alla normativa di volta in volta vigente.

Rapporti con la PA e rapporti con agenti e intermediari

Con riferimento ai rapporti con la PA e con gli agenti e intermediari, si rinvia al paragrafo 1.3 e 2.3.

4.4 Le procedure specifiche

Al fine di prevenire o ridurre al minimo il rischio di commissione delle fattispecie di reato rilevanti nello svolgimento delle attività sensibili, la Società ha adottato delle procedure specifiche che costituiscono parte integrante del presente Modello e a cui si fa integralmente rinvio, ed è certificata ai sensi di diverse Norme ISO, avendo adottato un Sistema di Gestione Integrato.

Di seguito sono elencate le principali procedure e certificazioni applicabili:

Certificazioni del Sistema di Gestione Integrato (SGI)
Maticmind ha implementato un Sistema di Gestione Integrato che soddisfa i requisiti di numerosi standard internazionali, garantendo la qualità dell'offerta, la sicurezza delle informazioni e la conformità normativa.

Certificazione/Normativa	Ambito di Applicazione	Dettagli
UNI EN ISO 9001:2015	Qualità	Copre la progettazione di sistemi e soluzioni, la commercializzazione, l'installazione, l'assistenza e la manutenzione di apparati e reti.
ISO/IEC 20000-1:2018	Service Management	Si applica all'installazione, all'assistenza, ai servizi di Network Operation Center (NOC) e Security Operation Center (SOC), ai servizi di Help Desk e alla consulenza IT.
UNI CEI ISO/IEC 27001:2022	Sicurezza delle Informazioni (SGSI)	Si applica alla fornitura di servizi NOC/SOC, consulenza in ambito di sicurezza, vulnerability assessment e penetration test, nonché allo sviluppo e manutenzione di sistemi software.
ISO/IEC 27017:2015 & 27018:2019	Sicurezza Cloud	Estensioni della ISO 27001 applicabili ai servizi Cloud e alla protezione dei Dati Personali Identificabili (PII) nei servizi Cloud pubblici.
UNI ISO 37001:2025	Anti-Corruzione	Il Sistema di Gestione Anticorruzione è certificato in conformità ai requisiti del D. Lgs. 231/2001.

Maticmind ha inoltre formalizzato le seguenti procedure che regolamentano il ciclo di vendita, dalla fase di identificazione dell'opportunità (pre-vendita) fino alla gestione dell'ordine e all'esecuzione delle commesse, a cui si fa integralmente rinvio:

- Progettazione Offerta di Vendita (PAQ820_1): descrive le attività per gestire l'offerta economico/commerciale verso il Cliente;

- Gestione Ordine di Vendita (PAQ820_2): dettaglia le attività di gestione di un Ordine Cliente e include il riesame dell'Ordine e la verifica della congruità con l'Offerta di Vendita;
- Gestione Gare di Appalto (PAQ820_3): regola le attività svolte per l'identificazione e la preparazione dei documenti relativi alla partecipazione a bandi di gara;
- Processo GonotGO_Gestione Proposte Commerciali: stabilisce le modalità di valutazione preventiva delle opportunità commerciali;
- Gestione Smart Licensing CISCO (IO720_1): descrive la gestione delle licenze Cisco nel processo di vendita e post-vendita inclusa l'individuazione dello smart account cliente e l'acquisto di licenze;
- Gestione Prodotti Dual Use (PAQ821_4): descrive l'iter di gestione degli aspetti relativi alla trade compliance per ordini e spedizioni di prodotti dual use.

5 SEZIONE 5: GESTIONE DELLA COMMESSA ED ESECUZIONE DEI PROGETTI

AREA A RISCHIO	ATTIVITÀ SENSIBILI	FUNZIONE COINVOLTA	REATI PRESUPPOSTO RILEVANTI
Progettazione e sales.engineering	- Interlocuzioni con clienti - Formulazione della soluzione tecnica ed economica	- Direzione Operations (COO) - KAM - TAM - Architetti - Direttori Operations BU - SE - Programmazione Gestione Lavori (PGL) - Aree Tecniche (PM/SM) - CISO - Direzione Compliace, Sustainability, Risk Management & Safety - Responsabile di Safety & Facility Management (Safety)	- Delitti informatici e trattamento illecito (art. 24 bis) - Corruzione e traffico di influenze illecite (art. 25) - Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni, introduzione nello Stato e commercio di prodotti con segni falsi (art. 25 bis) - Reati societari (art. 25 ter) - Intermediazione illecita e sfruttamento del lavoro (art. 25 quinquies) - Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 septies) - Reati in materia di violazione di misure restrittive dell'Unione europea (art. 25 octies 2) - Delitti in materia di violazione del diritto d'autore (art. 25 nonies) - Reati ambientali (art. 25 undecies) - Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25 duodecies)
Erogazione e gestione del servizio (execution.™. delivery)	- Definizione della pianificazione e ingaggio delle risorse - Monitoraggio dell'approvvigionamento dei materiali (OdA) da parte dell'Ufficio Acquisti - Installazione e configurazione degli apparati - Monitoraggio SAL e gestione dei Change - Registrazione delle ore spese per la consuntivazione - Esecuzione di Collaudo/Test formalizzato tramite Verbale di Collaudo (MIT) approvato dal cliente		
Logistica	- Gestione del magazzino e conservazione dei materiali - Gestione delle movimentazioni		
Assistenza e manutenzione (service. management)	- Gestione delle comunicazioni con i clienti - Gestione dei rapporti con i clienti		

	- Gestione degli interventi tecnici		

5.1 Alcuni esempi concreti dei Reati Presupposto rilevanti nella Gestione della commessa ed esecuzione dei progetti

Si riportano qui di seguito, a titolo esemplificativo, alcune delle potenziali condotte penalmente rilevanti che potrebbero verificarsi in relazione alle Aree di rischio sopra menzionate:

a) Reati informatici (art. 24 bis)

- attraverso l'accesso abusivo al sistema informatico di un cliente, la Società installa software finalizzati alla sottrazione di dati o informazioni rilevanti.

b) Delitto di intermediazione illecita e sfruttamento del lavoro (art. 25 quinquies)

- la Società affida la gestione del magazzino ad una cooperativa che impiega lavoratori in condizioni di sfruttamento.

c) Reati in materia di violazione di misure restrittive dell'Unione europea (art. 25 octies 2)

- la Società svolge servizi in favore di soggetti di nazionalità russa sanzionati o con sistemi localizzati in Russia.

5.2 Le regole generali di condotta nella Gestione della commessa ed esecuzione dei progetti

I Destinatari della presente Parte Speciale devono:

- operare nel rispetto delle leggi, regolamenti e normative vigenti, con particolare attenzione alla normativa in materia di sicurezza sul lavoro, tutela ambientale e anticorruzione;
- assicurare la corretta pianificazione e gestione della commessa, garantendo il rispetto di tempi, costi, qualità e obiettivi concordati con il Cliente;
- agire con trasparenza, integrità e lealtà, evitando ogni forma di favoritismo, conflitto di interesse, collusione o comportamento che possa compromettere l'imparzialità e l'indipendenza del progetto;
- garantire la tracciabilità delle decisioni e delle attività svolte nell'ambito della commessa, attraverso una documentazione chiara, completa e verificabile;
- astenersi dal richiedere o accettare, direttamente o indirettamente, somme di denaro, regali o altri vantaggi indebiti da parte di fornitori, Clienti, partner o altri soggetti interessati alla commessa, e adottare tutte le misure necessarie per prevenire fenomeni corruttivi, compresi controlli preventivi su controparti, tracciabilità dei flussi finanziari e segregazione delle funzioni;
- collaborare attivamente con le funzioni coinvolte nella progettazione fornendo tutte le informazioni richieste in modo tempestivo, accurato e completo;

- promuovere e favorire un ambiente di lavoro sicuro, rispettoso e professionale, contrastando qualsiasi forma di discriminazione, molestia o abuso di potere;
- selezionare fornitori mediante due diligence, verificando costantemente il rispetto dei CCNL e delle norme sul lavoro e monitorando le condizioni operative nei magazzini o negli eventuali ambienti cantieristici;
- preservare la riservatezza delle informazioni sensibili e dei dati personali acquisiti durante l'esecuzione del progetto, evitando divulgazioni non autorizzate;
- vietare qualsiasi accesso abusivo a sistemi informativi di Clienti, fornitori o terzi e l'installazione di software o strumenti non autorizzati nei sistemi di progetto;
- assicurarsi che ogni modifica progettuale, tecnica o contrattuale venga formalizzata, motivata e approvata secondo le procedure aziendali e contrattuali previste;
- contribuire al miglioramento continuo dei processi aziendali, condividendo le criticità riscontrate e le proposte di miglioramento a progetto concluso;
- garantire la tutela e il rispetto dei diritti di proprietà intellettuale e industriale di titolarità della Società o di terzi, utilizzando sempre software regolarmente licenziati, mantenendo un inventario delle licenze ed effettuando audit periodici;
- verificare Clienti, partner e destinazioni tramite screening sanzioni, assicurandosi di rispettare la normativa sui controlli di trade compliance.

5.3 Protocolli di condotta specifici

La progettazione dei prodotti e dei servizi venduti da Maticmind è un processo strutturato, in quanto la Società opera come System Integrator (SI), combinando prodotti di terze parti (Vendor) con soluzioni e servizi professionali propri per soddisfare le esigenze specifiche dei Clienti.

Questo processo rientra principalmente nelle attività di Pre-Vendita e Vendita.

Ruoli e strutture coinvolte nella progettazione

La progettazione è un'attività collaborativa che coinvolge diverse funzioni aziendali, ciascuna con responsabilità specifiche:

- Direzione Vendite (KAM/SE): il Key Account Manager (KAM) o Sales Executive (SE) è responsabile di raccogliere i requisiti e le esigenze del Cliente, identificando l'opportunità commerciale e avviando il processo di Pre-Vendita;
- Funzione Prevendita (Solution Engineering): questa funzione ha la responsabilità di formalizzare l'offerta economica e tecnica. Utilizza l'applicazione interna "Compositore di Offerta" (CDO) per elaborare il Piano Costi/Ricavi e la componente economica;
- Architetti e Specialisti Tecnici (Technical Account Manager – TAM): figure altamente specializzate supportano il KAM e la Prevendita nella progettazione di soluzioni complesse o innovative. Gli

Architect, in particolare, sono specialisti di architetture e prodotti, che possono avere una competenza avanzata su tecnologie specifiche e supportano la progettazione di architetture per Clienti Enterprise o Service Provider;

- Business Unit (BU): le Business Unit sono i riferimenti tecnologici della Società e contribuiscono con competenze specialistiche e know-how;
- Funzione CISO e DPO: il Chief Information Security Officer (CISO) approva le offerte specialistiche nel settore della sicurezza o che contengono un elevato contenuto di componenti/servizi di security. Il DPO (Data Protection Officer) è coinvolto per valutare gli aspetti di privacy e la conformità al GDPR.

Fasi e contenuti della progettazione

Il processo di progettazione garantisce che la soluzione proposta sia coerente con i requisiti del Cliente e che rispetti standard di qualità, economici e di conformità.

Raccolta dei requisiti e valutazione preliminare

- Registrazione: l'opportunità commerciale viene formalizzata nel Sistema Informativo Aziendale (SIM/Presales) con la creazione di una Scheda di Lavoro (SDL), che funge da contenitore per tutte le informazioni e i documenti relativi alla trattativa;
- analisi tecnica: la Prevendita analizza i requisiti del Cliente per individuare la soluzione ottimale, fornendo l'analisi di fattibilità e la stima della durata delle prestazioni.

Formulazione della soluzione tecnica ed economica

La soluzione proposta è una combinazione di:

- prodotti (HW/SW): acquisizione e integrazione di prodotti di Vendor leader del settore (come Cisco, Dell Technologies, Fortinet, etc.).
- servizi professionali: erogazione di servizi di configurazione, installazione, manutenzione, consulenza e supporto specialistico (ad esempio, servizi di cybersecurity);
- deliverable documentali: vengono elaborati documenti di progettazione tecnica, che possono includere disegni di alto livello (HLD) e di dettaglio (LLD) dell'infrastruttura.

Nella progettazione sono integrati elementi di compliance e sostenibilità:

- sostenibilità ambientale (ESG/DNSH): la progettazione tiene conto delle politiche dei Vendor per la sostenibilità ambientale (ad esempio, migrazione a soluzioni cloud-enabled o programmi di rigenerazione degli apparati - Takeback Incentive). Per i progetti PNRR, la Società assicura il rispetto del principio DNSH (Do No Significant Harm), estendendo tale verifica anche ai Vendor;
- gestione del rischio finanziario e fiscale: la Direzione Amministrazione è coinvolta per valutare l'esposizione finanziaria (fido del Cliente) e l'analisi dei bilanci della controparte per prevenire frodi o riciclaggio, specialmente per i nuovi Clienti.

Il risultato finale di queste fasi è l'emissione dell'Offerta di Vendita, che, se accettata dal Cliente, genera l'Ordine di Vendita (OdV) e avvia le attività di Delivery (Esecuzione) e Service Management (Assistenza e Manutenzione) gestite dalla Direzione Operations.

5.4 Le procedure specifiche

Al fine di prevenire o ridurre al minimo il rischio di commissione delle fattispecie di reato rilevanti nello svolgimento delle attività sensibili, la Società ha adottato delle procedure specifiche che costituiscono parte integrante del presente Modello e a cui si fa integralmente rinvio, ed è certificata ai sensi di diverse Norme ISO, avendo adottato un Sistema di Gestione Integrato.

Di seguito sono elencate le principali procedure e certificazioni applicabili:

Certificazioni del Sistema di Gestione Integrato (SGI)
Maticmind ha implementato un Sistema di Gestione Integrato (SGI) che soddisfa i requisiti di numerosi standard internazionali, garantendo la qualità dell'offerta, la sicurezza delle informazioni e la conformità normativa.

Certificazione/Normativa	Ambito di Applicazione	Dettagli
UNI EN ISO 9001:2015	Qualità	Copre la progettazione di sistemi e soluzioni, la commercializzazione, l'installazione, l'assistenza e la manutenzione di apparati e reti.
ISO/IEC 20000-1:2018	Service Management	Si applica all'installazione, all'assistenza, ai servizi di Network Operation Center (NOC) e Security Operation Center (SOC), ai servizi di Help Desk e alla consulenza IT.
UNI CEI ISO/IEC 27001:2022	Sicurezza delle Informazioni (SGSI)	Si applica alla fornitura di servizi NOC/SOC, consulenza in ambito di sicurezza, vulnerability assessment e penetration test, nonché allo sviluppo e manutenzione di sistemi software.
ISO/IEC 27017:2015 & 27018:2019	Sicurezza Cloud	Estensioni della ISO 27001 applicabili ai servizi Cloud e alla protezione dei Dati Personali Identificabili (PII) nei servizi Cloud pubblici.
UNI EN ISO 45001:2018	Salute e Sicurezza sul Lavoro (SSL)	Si applica alla progettazione di sistemi, alla commercializzazione, all'installazione, all'assistenza e alla manutenzione di apparati, e alle attività di logistica e magazzino.
UNI EN ISO 14001:2015	Gestione Ambientale (SGA)	Riguarda la progettazione di sistemi di telecomunicazione, la commercializzazione, l'installazione, la manutenzione e le attività di logistica e magazzino.

UNI EN ISO 14064-1:2019	Gas Serra (GHG)	Riguarda la quantificazione e la rendicontazione delle emissioni di gas ad effetto serra (GHG) e la loro rimozione.
UNI ISO 37001:2025	Anti-Corruzione	Il Sistema di Gestione Anticorruzione è certificato in conformità ai requisiti del D. Lgs. 231/2001.
UNI/PdR 125:2022	Parità di Genere	La certificazione è finalizzata a misurare e valutare i dati relativi al genere per colmare i gap e promuovere un cambiamento sostenibile.

I processi operativi di progettazione e delivery sono altresì supportati da procedure specifiche:

Progettazione e Offerta (design)

- Progettazione Offerta di Vendita (PAQ820_1): regola l'intero workflow di prevendita, dall'individuazione dell'esigenza alla formulazione dell'offerta economica/tecnica. Questa procedura include il processo di valutazione preliminare (Go/No-Go) delle opportunità commerciali per la Direzione Vendite Area Mercato, analizzando criteri economici e rischi, compresi quelli di compliance e di sicurezza.
- Gestione della Configurazione (PAQ852_2_CCA): per i progetti applicativi, definisce le modalità di identificazione e rintracciabilità dei Configuration Item (CI), la cui gestione è essenziale per l'integrità del sistema.

Erogazione e gestione del servizio (execution e delivery)

- Gestione Attività di Delivery (PAQ851_12): disciplina il Project Management delle attività di fornitura, installazione e configurazione, coprendo le fasi di Inizio, Pianificazione ed Esecuzione.
- Gestione del Service Management (PAQ851_12): regola la gestione dei servizi di Assistenza e Manutenzione (Assistance), basandosi sulla metodologia ITIL e assicurando il rispetto degli SLA (Service Level Agreement).
- Gestione Service Operation (PAQ851_12): descrive le attività delle strutture operative come Customer Care, NOC e SOC, relative alla gestione degli Incidenti (Incident Management), delle richieste (Request Fulfillment) e dei problemi (Problem Management).
- Gestione della Sicurezza negli Appalti (PAQ812_1): questa procedura è fondamentale per i servizi eseguiti in sedi esterne, stabilendo l'obbligo di richiedere al Cliente il Documento Unico di Valutazione dei Rischi Interferenziali (DUVRI) o il Piano di Sicurezza e Coordinamento (PSC) e, di conseguenza, di redigere il Documento di Valutazione dei Rischi Specifici (DRS) o il Piano Operativo di Sicurezza (POS).
- Gestione del Magazzino (PAQ854_1): regola le operazioni e le responsabilità relative alla gestione dei materiali in transito e in giacenza nei magazzini di Maticmind, in particolare per prevenire danni o deterioramenti durante stoccaggio, movimentazione e consegna.

- Politica Gestione Sicurezza Informazioni e Privacy Terze Parti (SGSI_P003): stabilisce i requisiti di sicurezza vincolanti per i fornitori e i subappaltatori che accedono ai sistemi o trattano informazioni per conto di Maticmind o dei suoi Clienti, coprendo aspetti organizzativi, fisici, tecnologici e di gestione del personale.
- Procedura Gestione Nomine AdS (GDPR_PR001): applicabile nel caso in cui il personale (interno o di terze parti) sia designato come Amministratore di Sistema (AdS), garantendo la conformità al Provvedimento del Garante Privacy per la gestione dei dati personali.
- Gestione Smart Licensing CISCO (IO720_1): fornisce istruzioni operative specifiche per la gestione centralizzata delle licenze software CISCO, un aspetto critico della fornitura tecnologica.

Per quanto riguarda le procedure più attinenti alla gestione del sistema informatico, si rinvia al paragrafo 7.3 sotto, mentre per quanto riguarda le procedure relative alla gestione degli aspetti relativi alla salute e sicurezza sul lavoro, si rinvia al paragrafo 8.2 sotto.

6 SEZIONE 6: PROCUREMENT

PROCESSI	ATTIVITÀ SENSIBILI	FUNZIONE COINVOLTA	REATI PRESUPPOSTO RILEVANTI
Selezione, qualifica e valutazione dei fornitori	- Selezione dei fornitori/consulenti - Gestione dell'albo fornitori/consulenti - Due.diligence e richiesta di documentazione ai nuovi fornitori/consulenti - Verifiche in materia di trade. compliance - Verifiche periodiche ai fornitore/consulenti	- ACQ - QSE - Direttore Operations (COO) - CFO - CM - Buyer - PMO - PS - PM	- Criminalità organizzata (art. 24 ter) e reati transnazionali (L. 146/2006) - Corruzione e traffico di influenze illecite (art. 25) - Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni, introduzione nello Stato e commercio di prodotti con segni falsi (art. 25 bis) - Reati societari (art. 25 ter) - Intermediazione illecita e sfruttamento del lavoro (art. 25 quinquies) - Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 septies) - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio (art. 25 octies) - Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (Art. 25 octies 1) - Reati in materia di violazione di misure restrittive dell'Unione europea (art. 25 octies 2)
Elaborazione e gestione degli ordini	- Richieste di acquisto - Elaborazione e trasmissione degli ordini - Monitoraggio degli acquisti/servizi ricevuti		

			- Reati tributari (art. 25 quinquiesdecies)

6.1 Alcuni esempi dei Reati Presupposto rilevanti per il Procurement

Si riportano qui di seguito, a titolo esemplificativo, alcune delle potenziali condotte penalmente rilevanti che potrebbero verificarsi in relazione alle Aree di rischio sopra menzionate:

a) Reati societari (art. 25 ter)

- nella selezione dei fornitori, un soggetto che agisce in nome e per conto di Maticmind pur avendo ricevuto più offerte competitive, favorisce sistematicamente un determinato fornitore che offre un prodotto qualitativamente inferiore o comunque non ottimale dietro pagamento di una tangente.

b) Reati tributari (art. 25 quinquiesdecies)

- nelle dichiarazioni IRES e IVA vengono indicati elementi passivi fittizi mediante l'utilizzo di fatture emesse da fornitori/consulenti a fronte di cessioni di beni/prestazioni di servizi inesistenti.

c) Delitti contro l'industria e il commercio (art. 25bis1)

- al fine di incrementare il margine economico, la Società procede all'acquisto e all'utilizzo di hardware difformi o di qualità inferiore rispetto a quanto contrattualmente pattuito, omettendo di informare il cliente e attestando falsamente la fornitura come conforme alle specifiche tecniche e qualitative previste.

6.2 Le regole generali di condotta nella fase di Procurement

I Destinatari della presente Parte Speciale devono:

- agire con trasparenza, imparzialità e correttezza in ogni fase del processo di approvvigionamento, assicurando parità di trattamento tra tutti i fornitori, attuali e potenziali;
- astenersi dal compiere, tollerare o favorire comportamenti illeciti, quali corruzione, concussione, favoritismi, collusioni o qualsiasi altra pratica che possa compromettere l'integrità del processo;
- astenersi dall'attivare forniture e/o consulenze senza garantirne congruità, adeguatezza e documentabilità e senza che vi siano effettive e obiettive esigenze della Società; in nessun caso, il conferimento di un ordine o un incarico di collaborazione/consulenza ovvero la selezione del terzo può essere motivata o condizionata da un qualsivoglia vantaggio improprio che possa ricevere la Società;
- rispettare scrupolosamente la normativa vigente, i regolamenti interni e le procedure aziendali relative agli acquisti, con particolare attenzione alla tracciabilità delle operazioni e alla documentazione delle decisioni prese;
- garantire che la fase di approvvigionamento sia improntata a un'adeguata segregazione delle funzioni tra il soggetto che manifesta l'esigenza, il soggetto che segue il processo di

aggiudicazione/negoziazione e contrattualizzazione, il soggetto che approva l'impegno di spesa e il soggetto che si occupa del controllo dell'esecuzione contrattuale;

- gestire con diligenza e riservatezza le informazioni relative alle gare, ai fornitori e ai contratti, evitando la divulgazione non autorizzata o l'uso improprio dei dati trattati;
- segnalare tempestivamente eventuali conflitti di interesse, anche potenziali, astenendosi dal partecipare a procedure di approvvigionamento in cui si ravvisi una situazione di incompatibilità personale o professionale;
- selezionare i fornitori sulla base di criteri oggettivi, quali qualità, affidabilità, prezzo, competenze tecniche e rispetto delle normative vigenti, escludendo ogni valutazione basata su rapporti personali o vantaggi indebiti;
- rifiutare ogni forma di omaggio, compenso, invito o altra utilità che possa influenzare o anche solo apparire in grado di influenzare l'imparzialità del processo decisionale;
- favorire la concorrenza e l'accesso al mercato, evitando pratiche discriminatorie o restrittive, e promuovendo la partecipazione di un ampio numero di operatori economici qualificati;
- regolare i rapporti con i fornitori esclusivamente attraverso ordini di acquisto e/o contratti/accordi scritti;
- consentire l'accesso ai dati anagrafici/identificativi degli operatori economici (i.e. ragione sociale, partita IVA, codice fiscale, coordinate bancarie) ai soli soggetti autorizzati;
- prevedere, nell'ambito degli ordini/contratti con i fornitori, per quanto applicabili, specifiche clausole di risoluzione e salvaguardia con riferimento:
  - all'inosservanza o violazione del Codice Etico e delle previsioni del Modello applicabili;
  - al mancato rispetto, per il personale impiegato nella prestazione, di tutte le misure previste a tutela della personalità individuale e del lavoratore, in materia di sicurezza e salute sul lavoro, regolarità contributiva e procacciamento di manodopera;
  - al mancato rispetto della normativa applicabile in materia di tutela ambientale;
  - al mancato rispetto della normativa applicabile in materia di tutela dei dati personali (privacy);
  - all'impiego di lavoratori non in regola con la normativa in materia di permesso di soggiorno;
  - all'obbligo di comunicare tempestivamente variazioni/modifiche dei dati, informazioni e documenti forniti, anche nell'ambito del processo di qualifica;
  - nell'acquisto di prodotti tutelati da diritti di proprietà intellettuale e industriale, all'attestazione di controparte:
    - di essere il legittimo titolare dei diritti di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o comunque di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;

- che i marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o di concessione in uso non violino alcun diritto di proprietà industriale in capo a terzi;
- circa l'impegno a manlevare e tenere indenne la Società da qualsivoglia danno o pregiudizio per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione.

6.3 I protocolli specifici di condotta

Il processo di approvvigionamento in Maticmind è gestito dalla Direzione Acquisti (ACQ) e rappresenta un insieme strutturato di attività che coprono l'identificazione del fabbisogno, la selezione dei fornitori, la negoziazione contrattuale e l'emissione degli ordini, con l'obiettivo di garantire efficienza, qualità e conformità normativa.

Tale processo è regolamentato da diverse procedure aziendali integrate nel Sistema di Gestione Integrato (SGI)

<u>Processo di approvvigionamento</u>

Il processo si articola nelle seguenti fasi principali:

1. Rilevazione del fabbisogno e richiesta di acquisto (RdA)

Il fabbisogno può essere generato da un Ordine di Vendita (OdV) già approvato (per la rivendita di prodotti/servizi) o da esigenze interne per investimenti (CAPEX) o spese operative (OPEX).

i. formalizzazione: per l'acquisto di servizi (inclusi servizi professionali, manutenzione o CAPEX/OPEX), la funzione richiedente (solitamente PMO della Direzione Operation) emette una Richiesta di Acquisto (RdA) tramite il sistema informativo aziendale (SIM/Presales), specificando l'oggetto e i requisiti;

ii. approvazione della spesa: l'RdA deve ottenere l'approvazione formale attraverso un workflow che segue livelli di delega definiti dalla Direzione (AD, CFO, Direttore Operation, etc.) in base all'importo della spesa;

iii. conformità codici: è un requisito vincolante che la RdA utilizzi codici articolo specifici per i servizi (come "-SER" o "-MAN") ed eviti codici generici per l'hardware (HW) al fine di garantire i corretti livelli di controllo e approvazione. La violazione di questa regola è sanzionabile;

2. Selezione del fornitore e negoziazione

Solo i fornitori presenti nell'Albo Fornitori con lo stato "Qualificato" o "Qualificato con riserva" possono essere utilizzati per l'emissione di ordini.

La qualifica è un processo attuato dalla funzione Supplier Evaluation & Rating (QSE) della Direzione Acquisti (DACQ). I fornitori sono classificati in classi (A, B, C) in base all'ordinato annuale. Sono soggetti a valutazione tutti i fornitori di servizi (A, B e C) e i fornitori di prodotti nazionali.

Il processo di qualifica avviene come segue:

Controlli in fase di selezione e qualifica

La selezione e l'inserimento nell'Albo Fornitori avvengono tramite la compilazione di un Questionario di Valutazione Fornitore (QVF) attraverso l'applicazione "Repository Albo Fornitori". I fornitori sono valutati per la loro idoneità (Qualificati) o con riserva (Qualificati con Riserva).

Le verifiche riguardano innanzitutto gli aspetti legali, amministrativi e reputazionali, ossia:

1. verifiche societarie: il fornitore deve fornire documentazione societaria aggiornata, inclusa la visura camerale (CCIAA) e gli ultimate beneficial owners (UBO);
2. conformità fiscale e contributiva: viene richiesta la Dichiarazione aggiornata di Regolarità Contributiva (DURC);
3. assenza di precedenti illeciti: vengono raccolte autocertificazioni e informazioni per accertare che il fornitore non sia stato oggetto di provvedimenti sanzionatori e/o cautelari ai sensi del Decreto o di tentativi di infiltrazione mafiosa (D. Lgs. 159/2011). Se esistono indagini penali o sanzioni 231, la società non procede alla qualifica;
4. antiriciclaggio: vengono verificati le modalità e le condizioni di pagamento per assicurare che non divergano dalla prassi commerciale.

Vengono in seguito verificate le capacità professionali e la conformità del sistema di salute e sicurezza sul lavoro:

1. qualificazione SSL: il fornitore è valutato per l'aderenza alle norme vigenti in materia di salute e sicurezza sul lavoro (D. Lgs. 81/08);
2. documentazione SSL: per l'erogazione di servizi in appalto o distacco, il fornitore deve mettere a disposizione documentazione che comprovi il rispetto degli obblighi in materia di SSL, inclusi: idoneità sanitarie (ove previste), attestati di formazione (generale e specifica), e il possesso di DPI;
3. verifica incidenti: viene chiesto al fornitore di confermare che negli ultimi cinque anni non si siano verificati incidenti mortali o invalidanti;
4. organizzazione sicurezza: è richiesta l'identificazione delle figure della sicurezza (Datore di Lavoro, RSPP, Medico Competente, RLS) e la copia delle relative nomine e attestati di formazione.

Vengono inoltre svolte verifiche con riferimento alla sicurezza delle informazioni e privacy (GDPR/SGSI)

1. gestione del rischio ICT: il fornitore deve aver definito e applicato un processo di Risk Management per identificare, analizzare e trattare sistematicamente i rischi per la sicurezza delle informazioni;
2. misure di sicurezza tecnologiche: vengono verificati i presidi di sicurezza (ad esempio hardening, anti-malware, sicurezza perimetrale) e la conformità con gli standard di sicurezza (ISO 27001);
3. privacy (GDPR): in caso di trattamento di dati personali, il fornitore deve dichiarare la conoscenza della normativa GDPR e garantire l'accettazione della nomina a responsabile del trattamento (Art. 28), oltre a garantire la nomina e la formazione degli amministratori di sistema (AdS);

4. sicurezza nella catena di fornitura: I requisiti di sicurezza devono essere definiti e concordati con ciascun fornitore, includendo la gestione della sicurezza nella catena di fornitura ICT.

La Società svolge infine verifiche in merito alla trade compliance, con riferimento a:

1. controllo delle liste di sanzioni, con la verifica che verifica che il fornitore (società, beneficiari effettivi, amministratori, intermediari) non compaia in:
   - liste UE;
   - liste OFAC;
   - liste ONU;
   - liste nazionali, ove applicabili.
2. verifica di liste di controllo export, al fine di evitare rapporti con soggetti coinvolti in proliferazione, terrorismo, violazioni dei diritti umani.
3. screening geografico, al fine di individuare i paesi soggetti a embargo totale o parziale e i paesi con restrizioni settoriali (come Russia, Iran, Corea del Nord).

La selezione del fornitore si basa su criteri oggettivi e imparziali come la competenza, le capacità tecniche (verificate dalla funzione PMO), l'affidabilità (anche finanziaria e reputazionale) e la competitività economica.

A seconda del tipo e dell'importo della fornitura, ACQ utilizza diverse metodologie:

- mono fornitura/semafori commerciali: (es. per Vendor predefiniti dal cliente);
- Request for Quotation (RFQ): (per l'acquisto di servizi complessi, richiedendo offerte ad almeno due fornitori);
- benchmark o procedura semplificata: (per forniture a basso impatto).

3. Stipula di accordi quadro e contratti

La stipula degli accordi è gestita dal Contract Manager (CM) o dal Buyer all'interno di ACQ.

Si utilizzano modelli contrattuali standard (accordo quadro o contratto di acquisto), composti dalle condizioni generali e dai seguenti allegati essenziali:

- allegato tecnico (specifiche di fornitura/servizio);
- allegato economico (prezzi unitari/corrispettivo totale);
- allegato sicurezza (adempimenti D. Lgs. 81/08);
- allegato nomina Responsabile del Trattamento (Art. 28 GDPR, se applicabile).

Ogni contratto deve includere la clausola 231 con l'impegno da parte del fornitore di rispettare il Modello Organizzativo e il Codice Etico di Maticmind.

I contratti firmati sono archiviati nel Repository Contratti (un'applicazione web) per garantirne la gestione controllata e la tracciabilità.

La delega per la firma degli accordi quadro o contratti (il documento principale) è divisa in base all'importo annuo della fornitura tra il Direttore Acquisti e l'Amministratore Delegato:

- per importi di ordinato annuo inferiori a € 500.000, la firma è di competenza del Direttore Acquisti;
- per importi di ordinato annuo superiori a € 500.000, la firma è di competenza dell'Amministratore Delegato.

4. Emissione dell'Ordine di Acquisto (OdA)

L'OdA è emesso da ACQ a valle dell'approvazione della RdA (se prevista).

- l'OdA è registrato nel sistema gestionale aziendale (SIM/Navision) e associato in modo univoco alla Scheda di Lavoro (SDL) e all'Ordine di Vendita;
- l'OdA deve essere firmato (con firma autografa o digitale) dal Buyer/Responsabile di Acquisti, seguendo i limiti di delega stabiliti.

La catena di approvazione per OdA e Contratti è progressiva: Responsabile Acquisti, Direttore Acquisti, Amministratore Delegato (AD).

5. Ricezione Merce e Servizi (EM/ES)

Per i beni fisici, il magazzino controlla la corrispondenza tra il Documento di Trasporto (DDT) e l'OdA su NAVision, registrando poi l'entrata a sistema.

Per i servizi, l'entrata viene registrata dall'Ufficio Amministrazione Contabilità Fornitori (ACF) o dai Project/Service Manager sulla base dell'effettiva erogazione

<u>Controlli e monitoraggio in corso di contratto</u>

Il monitoraggio dei fornitori qualificati è continuo e ha lo scopo di confermarne la permanenza nell'Albo Fornitori e garantire l'efficacia del servizio.

La Direzione Operation, tramite Project e Service Manager (PM/SM), monitora le prestazioni del fornitore, solitamente con cadenza annuale, compilando il Questionario di Valutazione dei Servizi (QVS). I criteri di valutazione includono:

- qualità tecnica e operativa: adeguatezza delle competenze del personale, disponibilità geografica delle risorse e rispetto delle tempistiche di fornitura/servizio;
- aderenza contrattuale: tempestività nella risposta alle richieste di offerta e uso del template standard di offerta Maticmind;
- compliance IT: rispetto dei requisiti e controlli di Sicurezza delle Informazioni (SGSI) specificati nell'accordo (come sicurezza fisica, sicurezza sul personale, Business Continuity e Disaster Recovery);

Maticmind si riserva il diritto di eseguire audit (internamente o tramite terze parti) per meglio valutare le prestazioni del fornitore. Tali audit possono essere condotti con un preavviso di 5 giorni o anche senza preavviso in caso di emergenza.

Gestione documentale e amministrativa

Maticmind assicura periodicamente:

1. aggiornamento continuo: la documentazione (DURC, CCIAA, attestati di formazione) viene monitorata con periodicità breve (3-6 mesi) e notifica al fornitore tramite il Repository dell'Albo Fornitori in caso di scadenza;
2. rinegoziazione contrattuale: in caso di inaffidabilità o peggioramento delle prestazioni, Maticmind può decidere di ridurre il coinvolgimento futuro del fornitore o escluderlo del tutto;
3. verifiche sul personale estero in distacco: in caso di lavoratori di paesi terzi impiegati in distacco o subappalto, Maticmind verifica e archivia regolarmente i documenti di identità e il permesso di soggiorno.

Obblighi alla cessazione del rapporto

Al termine del contratto, il fornitore è obbligato a:

1. restituire gli asset di Maticmind in suo possesso;
2. disabilitare gli accessi fisici e logici (utenze e credenziali);
3. fornire assistenza (passaggio di consegne) al subentrante, fornendo tutte le informazioni necessarie;
4. cancellare definitivamente tutti i dati personali raccolti durante il servizio.

6.4 Le procedure specifiche

Al fine di prevenire o ridurre al minimo il rischio di commissione delle fattispecie di reato rilevanti nello svolgimento delle attività sensibili, la Società ha adottato delle procedure specifiche che costituiscono parte integrante del presente Modello e a cui si fa integralmente rinvio, ed è certificata ai sensi di diverse Norme ISO, avendo adottato un Sistema di Gestione Integrato.

Di seguito sono elencate le principali procedure e certificazioni applicabili:

Certificazioni del Sistema di Gestione Integrato (SGI)
Maticmind ha implementato un Sistema di Gestione Integrato (SGI) che soddisfa i requisiti di numerosi standard internazionali, garantendo la qualità dell'offerta, la sicurezza delle informazioni e la conformità normativa.

Certificazione/Normativa	Ambito di Applicazione	Dettagli

UNI EN ISO 9001:2015	Qualità	Copre la progettazione di sistemi e soluzioni, la commercializzazione, l'installazione, l'assistenza e la manutenzione di apparati e reti.
UNI ISO 37001:2016	Anti-Corruzione	Il Sistema di Gestione Anticorruzione è certificato in conformità ai requisiti del D. Lgs. 231/2001.
UNI/PdR 125:2022	Parità di Genere	La certificazione è finalizzata a misurare e valutare i dati relativi al genere per colmare i gap e promuovere un cambiamento sostenibile.

I processi operativi di procurement sono altresì supportati da procedure specifiche:

- Gestione Documenti di Registrazione della Qualità (PAQ750_2) che stabilisce i criteri, le responsabilità e le modalità operative adottate da Maticmind per la gestione e il controllo della documentazione di registrazione della Qualità relativa al Sistema di Gestione Integrato (SGI);
- Gestione degli Approvvigionamenti (PAQ840_3) che definisce i criteri generali, le responsabilità e le modalità operative per l'acquisto di prodotti, servizi, opere (OPEX e CAPEX);
- Gestione dei Fornitori (PAQ840_1) che stabilisce i criteri e le modalità per la valutazione, la qualificazione e il monitoraggio dei fornitori e la tenuta dell'Albo Fornitori;
- Contract Management (PAQ840_2) che regola la preparazione, la negoziazione e la stipula di Contratti e Accordi Quadro (AQ) con i fornitori;
- Gestione Richiesta di Acquisto (PAQ851_9) che delinea il flusso per la formalizzazione interna delle esigenze di acquisto (RdA);
- SGI_Processo di Budgeting and Accounting Management, che regola il processo di pianificazione strategica dei ricavi e dei costi (budgeting) e la successiva gestione e contabilizzazione dei costi e dei servizi;
- MM_PAMM003_Fatturazione Passiva, che descrive le attività svolte per gestire il processo di fatturazione passiva specificando le funzioni aziendali coinvolte e le responsabilità operative di ciascuna delle funzioni e le relative applicazioni del sistema informativo aziendale;

7 SEZIONE 7: GESTIONE DEL SISTEMA INFORMATICO

PROCESSI	ATTIVITÀ SENSIBILI	FUNZIONE COINVOLTA	REATI PRESUPPOSTO RILEVANTI
Gestione e utilizzo dei sistemi informatici aziendali	- Gestione dei dispositivi e degli applicativi informatici e dei siti utili alla specifica funzione - Redazione e archiviazione di documenti informatici - Utilizzo, gestione e monitoraggio dei device aziendali - Gestione dei presidii di protezione per la cybersicurezza e per gestione della sicurezza delle informazioni - Gestione delle utenze e delle relative autorizzazioni - Formazione dei dipendenti in merito alla sicurezza informatica	- ICT Manager - CISO - SOC - Responsabile della Sicurezza delle Informazioni - Internal Auditor della Sicurezza - CSIRT (Computer. Security.Incident. Response.Team) - DPO - Utenti	- Delitti informatici e trattamento illecito di dati (art. 24 bis) - Reati societari (art. 25 ter) - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio (art. 25 octies) - Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25 octies 1) - Reati in materia di violazione di misure restrittive dell'Unione Europea (art. 25 octies.2) - Delitti in materia di violazione del diritto d'autore (art. 25 novies) - Reati tributari (art. 25 quinquiesdecies)

7.1 Alcuni esempi dei Reati Presupposto rilevanti nella Gestione del sistema informatico

Si riportano qui di seguito, a titolo esemplificativo, alcune delle potenziali condotte penalmente rilevanti che potrebbero verificarsi in relazione alle Aree di rischio sopra menzionate:

a) Reati societari (art. 25 ter)

- durante un'ispezione da parte delle autorità di vigilanza, vengono alterati i log del server per far risultare inesistenti alcune comunicazioni/corrispondenza rilevanti ai fini del controllo.

b) Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25 octies)

- al fine di ripulire denaro derivante da attività illecite, attraverso un sistema cloud gestito internamente, vengono creati wallet crypto intestati a terzi (fittizi) e viene suddiviso il contenuto dei wallet illeciti in microtransazioni ("smurfing").

c) Reati tributari (art. 25 quinquiesdecies)

- vengono implementate modifiche occulte ai software di contabilità per alterare l'effettiva registrazione delle fatture o dei ricavi (non registrare alcune fatture o registrarle in periodi successivi o generare fatture fittizie per aumentare i costi deducibili) e ridurre le imposte sul reddito o l'IVA dovuta.

7.2 Le regole generali di condotta nella Gestione del sistema informatico

I Destinatari della presente Parte Speciale devono:

- utilizzare i sistemi informatici e i dispositivi elettronici aziendali in modo conforme alla normativa vigente, alle policy interne e alle finalità strettamente connesse all'attività lavorativa, evitando ogni uso improprio, illecito o non autorizzato;
- adottare comportamenti improntati alla diligenza, correttezza, trasparenza e responsabilità nell'accesso, nella gestione e nella conservazione delle informazioni digitali, in particolare quelle contenenti dati personali, riservati, strategici o coperti da segreto industriale;
- evitare qualsiasi attività che possa comportare alterazione, distruzione, cancellazione, manipolazione non autorizzata o accesso abusivo ai sistemi informatici, sia interni che esterni all'azienda;
- rispettare le misure di sicurezza informatica definite dall'organizzazione, compreso:
  - l'uso corretto delle credenziali di accesso (user ID e password);
  - l'aggiornamento costante dei sistemi;
  - l'utilizzo autorizzato di software e dispositivi;
  - l'obbligo di segnalazione immediata di eventuali anomalie, incidenti di sicurezza o accessi non autorizzati;
- collaborare attivamente con l'ICT Manager, il Chief Information Security Officer e tutte le figure apicali responsabili nel monitoraggio, nella verifica e nell'aggiornamento delle infrastrutture tecnologiche e dei sistemi di difesa aziendali (es. antivirus, firewall, backup, logging);
- scaricare, elaborare o utilizzare materiale informatico in conformità con le norme in materia di diritti di proprietà intellettuale;
- evitare la diffusione di contenuti non conformi ai principi aziendali o lesivi della reputazione della Società, tramite strumenti informatici, e-mail, piattaforme collaborative, social network o qualsiasi canale digitale gestito dall'organizzazione;
- gestire con particolare attenzione i dati personali e sensibili, nel rispetto del Regolamento (UE) 2016/679 (GDPR), assicurando che ogni trattamento avvenga in base a criteri di minimizzazione, sicurezza, tracciabilità e legittimità;

- non installare o utilizzare software non autorizzati o non licenziati, in quanto ciò comporta gravi rischi legali, di sicurezza e di responsabilità per la Società;
- adottare comportamenti preventivi contro reati informatici e frodi digitali, come phishing, malware, ransomware o utilizzo indebito di strumenti informatici aziendali;
- favorire la cultura della sicurezza informatica e della protezione dei dati, partecipando alle attività di formazione e aggiornamento periodico promosse dalla Società.

7.3 Protocolli di condotta specifici e sistema di controllo per la sicurezza delle informazioni

Gestione del sistema di controllo per la sicurezza delle informazioni

Il Responsabile della Sicurezza delle Informazioni, con la collaborazione dei singoli Responsabili delle Funzioni aziendali 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. Partecipa inoltre ai Riesami periodici della Direzione.

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 GDPR e dalla normativa applicabile 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 GDPR e la normativa applicabile, nonché con 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 della Società 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.

Normativa NIS2 e DORA

La Società è soggetta alla normativa NIS 2 (Direttiva UE 2022/2555, recepita dal D.Lgs. 138/2024 e Legge 90/2024) per via del suo ruolo nel settore ICT come System Integrator e fornitore di servizi specializzati, in particolare per clienti che operano in settori critici e strategici.

Inoltre, la normativa DORA (Digital Operational Resilience Act - Regolamento UE 2022/2554) impatta direttamente Maticmind in quanto la Società funge da fornitore di istituti bancari, rendendo necessaria l'adesione a requisiti di sicurezza e resilience molto stringenti in ambito contrattuale e operativo.

Sebbene tali requisiti siano stati introdotti a tutela dell'integrità del proprio sistema informatico più che in chiave preventiva contro la commissione di Reati Presupposto, l'implementazione di tali misure si inserisce nel quadro generale dei presidi di controllo del sistema e rileva quindi anche ai fini 231.

La Società ha quindi avviato un processo di adeguamento agli obblighi normativi NIS2 e DORA, che prevede:

1. Adempimenti generali: Maticmind ha soddisfatto tutti gli adempimenti e le misure richieste in relazione alla direttiva NIS2, inclusi quelli richiesti tramite il portale dell'Agenzia per la Cybersicurezza Nazionale (ACN). Le nomine apicali richieste dalla normativa NIS2 sono dunque state effettuate, come la nomina del referente CSIRT (Computer Security Incident Response Team).
2. Formazione dei vertici aziendali: è stata effettuata la formazione obbligatoria per i soggetti apicali (come i membri del Consiglio di Amministrazione) in ambito NIS2 e DORA.

3. Integrazione documentale e processuale (SGSI): la Società ha integrato la Politica di Gestione della Sicurezza delle Informazioni e Privacy per le Terze Parti (MM_SGSI_P003) includendo i requisiti della Direttiva NIS2, come implementata dalla normativa italiana, al fine di supportare la conformità in materia di cybersecurity. Maticmind ha inoltre implementato la normativa DORA, negoziando le clausole contrattuali richieste dagli istituti bancari clienti, con l'obiettivo di valutare l'impatto economico delle modifiche richieste e sostenere i costi solo se giustificati o pagati dal cliente.

7.4 Le procedure specifiche

Al fine di prevenire o ridurre al minimo il rischio di commissione delle fattispecie di reato rilevanti nello svolgimento delle attività sensibili, la Società ha adottato delle procedure specifiche che costituiscono parte integrante del presente Modello e a cui si fa integralmente rinvio, ed è certificata ai sensi di diverse Norme ISO, avendo adottato un Sistema di Gestione Integrato.

Di seguito sono elencate le principali procedure e certificazioni applicabili:

Certificazioni del Sistema di Gestione Integrato (SGI)
Maticmind ha implementato un Sistema di Gestione Integrato che soddisfa i requisiti di numerosi standard internazionali, garantendo la qualità dell'offerta, la sicurezza delle informazioni e la conformità normativa.

Certificazione/Normativa	Ambito di Applicazione	Dettagli
UNI EN ISO 9001:2015	Qualità	Copre la progettazione di sistemi e soluzioni, la commercializzazione, l'installazione, l'assistenza e la manutenzione di apparati e reti.
ISO/IEC 20000-1:2018	Service Management	Si applica all'installazione, all'assistenza, ai servizi di Network Operation Center (NOC) e Security Operation Center (SOC), ai servizi di Help Desk e alla consulenza IT.
UNI CEI ISO/IEC 27001:2022	Sicurezza delle Informazioni (SGSI)	Si applica alla fornitura di servizi NOC/SOC, consulenza in ambito di sicurezza, vulnerability assessment e penetration test, nonché allo sviluppo e manutenzione di sistemi software.
ISO/IEC 27017:2015 & 27018:2019	Sicurezza Cloud	Estensioni della ISO 27001 applicabili ai servizi Cloud e alla protezione dei Dati Personali Identificabili (PII) nei servizi Cloud pubblici.

I processi di gestione e tutela del sistema informatico sono altresì supportati da procedure specifiche, di fatto trasversali a più Aree di rischio della Società, e dunque già in parte richiamate nelle rispettive sezioni;

ad esempio, le procedure Gestione Attività di Delivery (PAQ851_12) e Gestione della Configurazione (PAQ852_2_CCA), richiamate sopra, regolano le attività di delivery e configurazione anche negli aspetti informatici. Per quanto riguarda le procedure più inerenti alla gestione informatica, e facenti parte del SGSI, si richiamano dunque, con rinvio integrale ai rispettivi contenuti, le seguenti procedure:

- Procedura Sicurezza Logica (SGSI_PR005): definisce le modalità operative per la gestione della sicurezza logica del sistema informativo di Maticmind, coprendo aspetti come il ciclo di vita delle utenze, la gestione delle password, l'accesso alle risorse, l'uso della posta elettronica e dei dispositivi portatili, ed è un documento di riferimento per la prevenzione dei delitti informatici. È corredata dalla Politica di Sicurezza Logica (SGSI_P005), che stabilisce gli indirizzi e le regole di alto livello per la sicurezza logica di Maticmind, assicurando che l'accesso alle informazioni e alle risorse sia controllato in base ai requisiti aziendali e di sicurezza.
- Procedura Sicurezza Logica Cliente: documento di riferimento per la gestione e la prevenzione dei reati informatici nell'ambito delle attività di Maticmind, specificamente per quanto riguarda la sicurezza logica relativa ai clienti. È a sua volta corredata dalla Politica Sicurezza Logica Cliente, documento di riferimento per la gestione della sicurezza logica quando le attività di Maticmind coinvolgono i sistemi dei clienti.
- Gestione del Service Management (PAQ851_12): regola la gestione dei servizi di Assistenza e Manutenzione (Assistance), basandosi sulla metodologia ITIL e assicurando il rispetto degli SLA (Service Level Agreement).
- Politica Gestione Sicurezza Informazioni e Privacy Terze Parti (SGSI_P003): stabilisce i requisiti di sicurezza vincolanti per i fornitori e i subappaltatori che accedono ai sistemi o trattano informazioni per conto di Maticmind o dei suoi Clienti, coprendo aspetti organizzativi, fisici, tecnologici e di gestione del personale.
- Procedura Gestione Nomine AdS (GDPR_PR001): applicabile nel caso in cui il personale (interno o di terze parti) sia designato come Amministratore di Sistema (AdS), garantendo la conformità al Provvedimento del Garante Privacy per la gestione dei dati personali.
- Gestione Smart Licensing CISCO (IO720_1): fornisce istruzioni operative specifiche per la gestione centralizzata delle licenze software CISCO, un aspetto critico della fornitura tecnologica.

8 SEZIONE 8: GESTIONE DEGLI ADEMPIMENTI RELATIVI A SALUTE E SICUREZZA SUL LAVORO E ALLA GESTIONE AMBIENTALE

PROCESSI	ATTIVITÀ SENSIBILI	FUNZIONE COINVOLTA	REATI PRESUPPOSTO RILEVANTI
Pianificazione e organizzazione dei ruoli e delle attività connesse alla tutela della salute, della sicurezza e igiene sul lavoro	- Definizione del sistema aziendale di sicurezza (ruoli, responsabilità, deleghe) - Nomina e aggiornamento dei soggetti obbligati (Datore di Lavoro, RSPP, ASPP, medico competente, RLS, dirigenti e preposti) - Predisposizione del DVR e dei documenti valutativi correlati - Nomina, revoca e verifica di idoneità delle figure interne della sicurezza - Verifica dei requisiti di competenza/formazione delle figure interne (RSPP, RLS, preposti, ecc.)	- Datore di lavoro - RSPP - Preposti - RU - RLS - Medico competente - Direzione Compliace, Sustainability, Risk Management & Safety - Responsabile di Safety & Facility Management (Safety) - Project Manager (PM) / Service Manager (SM) - Magazzino e Logistica (MGZ) - Mobility Manager	- Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24) - Delitti di criminalità organizzata (art. 24 ter) e reati transnazionali (L. 146/2006) - Corruzione e traffico di influenze illecite (art. 25) - Reati societari (art. 25 ter) - Intermediazione illecita e sfruttamento del lavoro (art. 25 quinquies) - Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 septies) - Reati ambientali (art. 25 undecies)
Attività di informazione e formazione in tema di salute, sicurezza e igiene sul lavoro	- Progettazione e aggiornamento dei programmi formativi - Erogazione, registrazione e verifica dell'efficacia della formazione e informazione obbligatoria - Tracciamento delle presenze e aggiornamenti periodici		
Gestione dei rischi in tema di salute,	- Redazione e aggiornamento del Documento di		

sicurezza e igiene sul lavoro	Valutazione dei Rischi (DVR) - Identificazione, valutazione e aggiornamento dei rischi specifici (es. chimici, elettrici, rumore, biologico, ecc.) - Adozione e verifica delle misure di prevenzione e protezione - Monitoraggio della sorveglianza sanitaria - Gestione degli infortuni		
Gestione dell'emergenza e del Primo Soccorso	- Nomina e formazione degli addetti alle emergenze (antincendio, primo soccorso, evacuazione) - Redazione e aggiornamento del piano di emergenza aziendale - Esecuzione di prove di evacuazione, test antincendio, e aggiornamento procedure		
Rapporti con i fornitori con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro	- Qualifica dei fornitori/subappaltatori in base ai requisiti di sicurezza - Verifica della documentazione (DUVRI, POS, attestati formazione, DURC) - Controlli e audit sui comportamenti dei fornitori in cantiere o presso la sede operative		

Gestione ambientale	- Gestione dello smaltimento dei rifiuti; - Controllo e gestione del parco auto aziendale e della flotta		

8.1 Alcuni esempi dei Reati Presupposto rilevanti per gli adempimenti in materia di salute e sicurezza sul luogo di lavoro e di gestione ambientale

Si riportano qui di seguito, a titolo esemplificativo, alcune delle potenziali condotte penalmente rilevanti in relazione alle Aree di rischio sopra menzionate:

a) Corruzione e traffico di influenze illecite (art. 25)

- vengono offerti o promessi denaro o altra utilità a un soggetto che ha o asserisce di avere rapporti con un pubblico ufficiale o un incaricato di pubblico servizio, al fine di ottenere vantaggi con la sua intermediazione (es. ignorare eventuali inadempimenti/non conformità di Maticmind alla normativa vigente in materia di salute e sicurezza sul lavoro).

b) Reati societari (art. 25 ter)

- vengono offerti o promessi – anche per interposta persona – denaro o altra utilità non dovuti ad un soggetto facente parte della struttura societaria dell'ente certificatore, al fine di ottenere uno dei certificati per gli standard nazionali, nonostante Maticmind non detenga le caratteristiche/requisiti per il rilascio dello stesso.

c) Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 septies)

- si verifica un infortunio a causa del mancato aggiornamento del documento di valutazione dei rischi e della conseguente mancata erogazione della formazione in merito al rischio non aggiornato.

8.2 Le regole generali di condotta in materia di salute e sicurezza sul luogo di lavoro e di gestione ambientale

Per tutti i Destinatari del Modello è vietato:

- porre in essere comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, fattispecie di reato rientranti tra quelle sopra considerate (art. 25 septies e art. 25 undecies del Decreto);
- porre in essere comportamenti imprudenti, negligenti od imperiti che possano costituire un pericolo per la sicurezza all'interno dei luoghi di lavoro;
- rifiutare di utilizzare dispositivi di protezione individuale o collettivi o svolgere attività lavorative in violazione delle disposizioni impartite dai responsabili per la sicurezza;

- svolgere attività di lavoro e adoperare macchinari e strumentazioni senza aver preventivamente ricevuto adeguate istruzioni sulle modalità operative oppure senza aver precedentemente partecipato a corsi di formazione;
- omettere la segnalazione della propria eventuale incapacità o inesperienza nell'uso di strumenti aziendali;
- rifiutarsi di partecipare a corsi di formazione in materia di salute e sicurezza sul luogo di lavoro;
- alterare, modificare e/o manomettere i sistemi di protezione individuale e/o sistemi di protezione installati sugli strumenti di lavoro;
- utilizzare e/o far utilizzare macchinari e/o strumenti che non siano in buono stato manutentivo o che non abbiano subito le validazioni richieste per legge, ove necessarie.

Con riferimento alla gestione ambientale, la Società impone a tutti i Destinatari l'obbligo di:

- osservare i dettami previsti da leggi e regolamenti in materia ambientale;
- osservare le politiche, i protocolli e le procedure che disciplinano l'attività aziendale, con riferimento, in particolare, a quanto regolamentato dal Modello;
- astenersi dal compiere di propria iniziativa operazioni o manovre che non rientrino nelle proprie mansioni o, comunque, che siano suscettibili di recare danni all'ambiente;
- segnalare tempestivamente all'organo amministrativo eventuali situazioni di pericolo e di rischio per l'ambiente, ovvero situazioni di emergenza ambientale;
- partecipare alle sessioni formative e di addestramento organizzate dalla Società in materia di tutela ambientale;
- conservare tutta la documentazione relativa al rispetto delle prescrizioni in materia ambientale prevista da norme di legge o da autorizzazioni amministrative.

Ai Destinatari è fatto altresì espresso divieto, in particolare, di:

- abbandonare o depositare in modo incontrollato i rifiuti;
- conferire l'attività di gestione dei rifiuti a soggetti non dotati di apposita autorizzazione per il loro smaltimento e recupero;
- abbandonare o depositare in modo incontrollato i rifiuti o immetterli, allo stato solido o liquido;
- conferire l'attività di gestione dei rifiuti a soggetti non dotati di apposita autorizzazione per il loro smaltimento e recupero;
- miscelare categorie diverse di rifiuti pericolosi e non pericolosi;
- violare gli obblighi di comunicazione e documentazione per la gestione dei rifiuti, ovvero falsificare/ alterare tale documentazione;

- realizzare scarichi di sostanze ed emissioni in atmosfera in violazione delle prescrizioni normative e/o delle autorizzazioni ricevute o, comunque, in modo tale da causare danni all'ambiente e mettere in pericolo la salute della collettività interessata.

A) Adempimenti in materia di salute e sicurezza sul lavoro

Con riferimento alla gestione degli adempimenti in materia di salute e sicurezza sul lavoro, Maticmind ha adottato un sistema di gestione della salute e sicurezza pienamente conforme ai requisiti di cui all'art. 30 del D.lgs. 81/2008 (o "TUS") e alla Norma UNI EN ISO 45001:2018 (Sistemi di gestione per la salute e la sicurezza sul lavoro), che stabilisce i requisiti per un sistema di gestione mirato a prevenire infortuni e malattie professionali.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, i Destinatari sono tenuti, in generale, a rispettare tutte le regole e i principi contenuti nei seguenti documenti, per le parti di proprio interesse:

- Documenti di valutazione dei rischi:
  - Tomo 1: Rischi legati ai Luoghi di Lavoro (DVR_T1_Rischi Luoghi Lavoro): descrive l'organizzazione della sicurezza, i rischi trasversali (ad esempio, rischio incendio, rischio biologico, microclima) e le modalità di valutazione dei rischi per i siti esterni;
  - Tomo 2: Rischi della Mansione (DVR_Rischi legati alla Mansione): contiene la valutazione dei rischi specifici per mansione, come l'esposizione al lavoro al videoterminale, il lavoro notturno, il lavoro in solitaria e lo stress lavoro-correlato (SLC);
  - DVR specifici per ciascuna sede.
- Documenti specifici per la gestione degli appalti: procedura Gestione della Sicurezza negli Appalti (PAQ812_1): regola la gestione della sicurezza quando Maticmind opera presso le sedi dei Clienti (attività fuori sede) e definisce i seguenti documenti fondamentali:
  - DUVRI (Documento Unico per la Valutazione dei Rischi Interferenziali) / PSC (Piano di Sicurezza e Coordinamento): documenti richiesti al Cliente per la valutazione dei rischi di interferenza. Il PSC è richiesto per i cantieri (Titolo IV), mentre il DUVRI è richiesto per gli ambiti non cantieristici;
  - DRS (Documento di Valutazione dei Rischi Specifici): è il documento redatto da Maticmind (o, in caso di subappalto, dal fornitore) per le attività in ambito non cantieristico. Viene preparato dal RSPP di Maticmind basandosi sul DUVRI del Cliente e sulle informazioni tecniche raccolte dal Project Manager (PM) Preposto;
  - POS (Piano Operativo di Sicurezza): è il documento redatto da Maticmind per le attività svolte nei cantieri (Titolo IV), basandosi sul PSC fornito dal Cliente.

    Per l'integrazione o la modifica di tali documenti in assenza di variazioni dei rischi interferenziali, si fa riferimento al documento "Integrazione ai Documenti DRS o POS".
- Documentazione organizzativa (organigrammi e ruoli);
- Procedure e piani di formazione e controllo (piani di miglioramento):

- Piano di formazione per addetti SSL (PAQ622_1): documento che formalizza e pianifica la formazione trasversale obbligatoria (generale, specifica e specialistica);
- Gestione sorveglianza sanitaria (PAQ712_3): procedura che definisce l'attività di Sorveglianza Sanitaria svolta dal Medico Competente (MC);
- Gestione dispositivi protezione individuale (PAQ813_2): regolamenta la scelta, l'approvvigionamento e l'assegnazione dei DPI ai dipendenti, come scarpe antinfortunistiche, guanti, ecc., che sono obbligatori in caso di intervento in cantiere (Titolo IV);
- Gestione lavoro in solitaria (IO813_1_SSL_T2): istruzione operativa per gestire e monitorare il rischio per i tecnici che operano in isolamento;
- Piani di gestione delle emergenze (PGE): contenuti all'interno dei DVR di sede, descrivono le procedure da attuare in caso di incendio o sisma;
- Gestione near miss (PAQ813_1_SSL_T1): la Società utilizza tale procedura per raccogliere segnalazioni strutturate di incidenti mancati, utili per l'analisi e l'individuazione di azioni di miglioramento per la prevenzione dei rischi;
- Gestione del Magazzino (PAQ854_1): regola le operazioni e le responsabilità relative alla gestione dei materiali in transito e in giacenza nei magazzini di Maticmind, in particolare per prevenire danni o deterioramenti durante stoccaggio, movimentazione e consegna.
- Allegato 4: modulo utilizzato dal Project Manager Preposto per la raccolta di informazioni per la valutazione rischi, a supporto del RSPP nella redazione di DRS o POS. Funge dunque da strumento di controllo per verificare la validità di idoneità sanitarie e attestati di formazione.

- piano sanitario e documentazione relativa alla sorveglianza sanitaria del personale;
- Piano di Gestione delle Emergenze (PGE);
- Piano di Emergenza Coordinato (PEC).

Tutta la documentazione SSL è consultabile sul Portale SGI. I documenti relativi alla sicurezza e salute sul lavoro sono considerati documenti pubblici. La documentazione più specifica e personale (come le idoneità sanitarie e i dati relativi alle presenze) è invece gestita dalla funzione Risorse Umane (RU), la quale è responsabile di supportare il PM/SM nel reperire gli attestati di formazione e le idoneità sanitarie per il personale impiegato in appalto o distacco.

In ogni caso, Maticmind dovrà svolgere le proprie attività secondo i seguenti principi procedurali specifici:

- responsabilizzazione dell'intera organizzazione aziendale, dal datore di lavoro ai sensi del D.lgs. 81/2008 ("Datore di Lavoro") a ciascuno dei lavoratori nella gestione del sistema di salute e sicurezza sul lavoro, ciascuno per le proprie attribuzioni e competenze, al fine di evitare che l'attività di prevenzione venga considerata di competenza esclusiva di alcuni soggetti con conseguente mancanza di partecipazione attiva da parte di taluni Destinatari;

- impegno a considerare il sistema di salute e sicurezza come parte integrante della gestione aziendale, la cui conoscibilità deve essere garantita a tutti i Destinatari;
- impegno al miglioramento continuo ed alla prevenzione, nonché a monitorare in maniera costante la situazione e le relative azioni correttive/formative;
- impegno a garantire che ciascun Destinatario, nei limiti delle rispettive attribuzioni, sia sensibilizzato e formato per svolgere i propri compiti nel rispetto delle norme sulla tutela della salute e sicurezza sul lavoro;
- impegno al coinvolgimento ed alla consultazione dei lavoratori, anche attraverso il proprio rappresentante dei lavoratori per la sicurezza (RLS); in particolare, Maticmind definisce le modalità adeguate a realizzare il coinvolgimento dei lavoratori, anche attraverso il proprio RLS, per attuare la consultazione preventiva in merito all'individuazione e valutazione dei rischi e alla definizione delle misure preventive nonché riunioni periodiche con gli stessi;
- impegno a promuovere la collaborazione con le autorità competenti (ad es. INAIL, ASL, ecc.) al fine di stabilire un efficace canale di comunicazione rivolto al miglioramento continuo delle prestazioni in tema di sicurezza e tutela della salute dei lavoratori.

Per ogni requisito di cui all'art. 30 del TUS, si procederà ad illustrare le attività svolte da Maticmind in materia.

1) L'art. 30, lett. a) e b) del D.lgs. 81/2008

L'art. 30, lett. a) e b) del TUS prevede che il Modello può avere una valenza esimente se è assicurato l'adempimento di tutti gli obblighi giuridici relativi:

- al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti.

Preliminarmente alla definizione degli obiettivi specifici in materia di salute e sicurezza sul lavoro, Maticmind dovrà, pertanto, correttamente identificare i requisiti richiesti in tale ambito da leggi e regolamenti comunitari, nazionali, regionali e locali, anche al fine di garantire una corretta predisposizione ed implementazione del sistema di gestione della salute e sicurezza dei lavoratori.

Al fine di dare attuazione alla politica di cui al sopra, pertanto, il Datore di Lavoro, di concerto con il RSPP:

- definisce gli obiettivi finalizzati al mantenimento e al miglioramento del sistema, nonché le relative risorse, anche economiche, necessarie;
- definisce le modalità per il raggiungimento di ciascun obiettivo, individuando le figure/strutture coinvolte e l'attribuzione dei relativi compiti e responsabilità;
- prevede le modalità di verifica dell'effettivo ed efficace raggiungimento degli obiettivi;

- analizza ogni aspetto della salute e sicurezza disciplinato dal legislatore, utilizzando eventuali banche dati esistenti, documenti di associazioni imprenditoriali, sindacali, etc.;
- individua le disposizioni normative che interessano Maticmind sulla base dell'attività svolta;
- procede all'individuazione dei requisiti e degli adempimenti derivanti dal rispetto di tali norme applicabili all'attività svolta da Maticmind.

Con riferimento all'attività di valutazione dei rischi, Il Datore di Lavoro ha provveduto alla valutazione di tutti i rischi con la conseguente elaborazione del documento di valutazione dei rischi previsto dall'art. 28, TUS per ogni sede della Società:

Sede	Indirizzo	Attività principali	Dettagli aggiuntivi sulle attività
Roma	Via Mario Carucci 131	Direzione, Commerciale, Tecnica, Amministrativa, NOC, SOC	Sede amministrativa e operativa. Ospita il NOC (Network Operation Center) e il SOC (Security Operation Center). Il SOC fornisce servizi di monitoraggio di detection e response operanti 24/7.
Milano	Via Roberto Bracco 6 (Sede Legale)	Direzione, Commerciale, Tecnica, Amministrativa.	Sede legale e di direzione. Vengono svolte attività di produzione, costruzione e vendita di impianti radiotelevisivi ed elettronici in genere, nonché installazione e manutenzione di apparati e sistemi elettrici ed elettronici. Il NOC ha una presenza in questa sede.
Modena	Via Ferdinando Magellano 1	Commerciale, Tecnica, Logistica, Amministrativa	Sede tecnica e commerciale. Ospita un magazzino scorte, e funge da Solution Center/Show Room per demo ai Clienti. Il NOC ha una presenza qui.
Napoli	Via F. Lauria D4	Commerciale, Tecnica, Amministrativa	Sede dell'Enterprise Competence Center Applicativo (CCA) dove si eseguono attività relative a sviluppo e manutenzione di applicazioni software.
Torino	C.so Unione Sovietica 612/15c	Direzione, Commerciale, Tecnica	Il NOC ha una presenza in questa sede.
Padova	Galleria Spagna 28	Commerciale, Tecnica, Amministrativa	Sede in cui si svolge attività d'ufficio tecnico/amministrativa, inclusa la gestione di un magazzino scorte.
Sesto Fiorentino (FI)	Via A. Avogadro 34	Commerciale, Tecnica	Sede con attività intellettuali che ospita funzioni Commerciali e Tecniche (Delivery & Operation). Dispone di un locale adibito a magazzino scorte.
Massa Carrara	Via degli Oliveti 110	Tecnica, SOC.	Sede del SOC, dove si svolgono attività di monitoring, installazione, manutenzione on-site e a distanza di impianti di trasmissione dati e similari.

Ciampino (RM)	Via A. Segni 18/20	Logistica	Costituisce il polo logistico aziendale principale per lo stoccaggio dei prodotti destinati ai clienti e scorte tecniche. Ospita il magazzino vendite e il magazzino scorte.
Bari	Via Roma 12 / Modugno	Commerciale, Tecnica. Può includere funzioni Amministrative e Logistiche (nuove sedi ex CloudMind)	Sede in cui si svolgono attività di installazione, cablaggio, configurazione e manutenzione on-site e a distanza di impianti di trasmissione dati e similari, oltre ad attività commerciali.
San Giovanni La Punta (CT)	Via Cristoforo Colombo 13	Commerciale, Tecnica	Sede con attività commerciali (acquisizione dei contratti) e tecniche (installazione, programmazione e manutenzione).

Maticmind ha inoltre identificato i rischi comuni e specifici per la sicurezza e la salute, nonché le categorie di lavoratori esposte a tali rischi. I DVR si suddividono in due tomi principali: il Tomo 1 (Rischi legati ai Luoghi di Lavoro), che valuta i rischi trasversali e ambientali comuni a tutte le sedi, e il Tomo 2 (Rischi legati alla Mansione), che analizza i rischi specifici per ciascuna categoria professionale.

I rischi comuni a tutte le mansioni (fattori trasversali e ambientali), nelle sedi di Maticmind (uffici, laboratori e magazzini) sono:

Categoria di rischio	Livello di rischio	Dettagli sui pericoli
rischio elettrico	accettabile o basso	Rischi dovuti a contatti diretti/indiretti, propagazione di incendi o fulminazione. È ritenuto accettabile perché gli impianti sono a norma (DM 22/01/2008 n.37) e marcati CE.
rischio ambientale/igienico	basso o accettabile	Include microclima (temperatura, umidità), illuminazione e pulizia generale dei locali. Generalmente ritenuto basso poiché le condizioni microclimatiche e di illuminazione sono adeguate agli standard d'ufficio, e vengono effettuate manutenzioni periodiche agli impianti di condizionamento.
rischio biologico	accettabile	Rischio di infezioni virali (es. influenzali) e batteriche (es. legionella). Ritenuto accettabile con la raccomandazione di buona igiene delle mani e manutenzione/sanificazione regolare degli impianti di condizionamento e raffreddamento.
radiazioni non ionizzanti	accettabile	Rischio da apparecchiature come computer, Wi-Fi e lettori RFID. Ritenuto accettabile, ma è richiesta cautela per i lavoratori portatori di dispositivi medici impiantati (AIMD).
rischio sismico	basso o medio	La classificazione del rischio varia a seconda della sede (ad esempio, Basso a Milano e Torino; Medio a Roma e Napoli). Sono previste misure di gestione delle emergenze, tra cui l'evacuazione e il divieto di usare l'ascensore in caso di scossa.

Le categorie di lavoratori individuate per mansioni omogenee sono sette, con i seguenti rischi specifici:

categoria di lavoratori/mansione	rischi rilevanti e classe (rischio residuo)	DPI obbligatori
Personale Commerciale	Stress Lavoro Correlato (SLC): Basso. Lavoro al videoterminale (VDT): Accettabile. Lavoro in itinere: Basso.	Nessuno
Personale Amministrativo	SLC: Basso. VDT: Accettabile.	Nessuno
Project & Service Manager (PM/SM)	VDT: Accettabile. SLC: Basso. Lavoro in Itinere: Basso.	Nessuno
Programmatori	VDT: Accettabile. Lavoro in itinere: Basso. SLC: Basso.	Nessuno
Tecnici Installatori e Sistemisti	VDT: Accettabile. Lavoro in itinere: Basso. Lavoro in quota: Rischio trattato specificamente.	Obbligatori in caso di intervento in cantiere: casco, scarpe antinfortunistiche/isolanti, giubbotto luminescente.
Customer Care, NOC e SOC	VDT: Accettabile. Rischio Rumore (per l'uso delle cuffie): Medio Basso, con rischio di shock acustico gestito tramite sorveglianza sanitaria e cuffie specifiche. Lavoro notturno: Basso (principalmente reperibilità).	Nessuno.
Magazzinieri	Movimentazione Manuale dei Carichi (MMC): Basso. Caduta dall'alto: Accettabile. Esposizione a Vibrazioni/Rumore (muletto): Basso, ma soggetti a Sorveglianza Sanitaria.	Obbligatori: guanti, mascherina, scarpe antinfortunistiche, giubbino luminescente, occhiali (vicino alla stazione di ricarica del muletto), scale adeguate.
Lavori in quota e solitaria: per i tecnici installatori e i magazzinieri, sono rilevanti i rischi di caduta dall'alto e di movimentazione manuale dei carichi. I lavori in quota (oltre 2 metri) comportano formazione specifica e l'uso di DPI specifici. il lavoro in solitaria (soprattutto notturno per gli interventi di manutenzione) è un rischio a cui sono esposti i tecnici itineranti, ed è gestito attraverso procedure che prevedono l'obbligo di segnalare arrivo e partenza dal sito del cliente all'operatore NOC o al preposto.		

2) L'art. 30, lett. c) del D.lgs. 81/2008

L'art. 30, lett. c) del TUS concerne gli obblighi giuridici riguardanti le attività di natura organizzativa (quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza): il comma 3 dell'art. 30 prevede infatti che "il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla

natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".

L'assetto della struttura interna è meglio descritto nella Parte Generale del presente Modello.

Si riportano qui di seguito gli adempimenti che, in attuazione dei principi sopra descritti e della normativa applicabile, sono posti a carico delle figure rilevanti.

Il Datore di Lavoro

Al Datore di Lavoro sono attribuiti tutti gli obblighi in materia di salute e sicurezza sul lavoro, tra cui i seguenti non delegabili:

1) valutare, anche nella scelta delle attrezzature di lavoro e delle sostanze o dei preparati chimici impiegati, nonché nella sistemazione dei luoghi di lavoro, tutti i rischi per la sicurezza e per la salute dei lavoratori, ivi compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari; a tal proposito, nella scelta operata, il Datore di Lavoro dovrà garantire il rispetto degli standard tecnico strutturali previsti dalla legge, ed elaborare, all'esito di tale valutazione, un Documento di Valutazione dei Rischi;
2) designare il Responsabile del Servizio di Prevenzione e Protezione.

Il servizio di prevenzione e protezione (SPP)

Nell'adempimento degli obblighi in materia di salute e sicurezza sul lavoro, il Datore di Lavoro organizza il SPP all'interno dell'azienda o incarica persone o servizi esterni assicurandosi che il RSPP, da questi nominato, sia in possesso delle capacità e dei requisiti professionali di cui all'art. 32 del TUS.

Il RSPP provvede a:

- individuare i fattori di rischio, valutare i rischi ed individuare le misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
- elaborare, per quanto di competenza, le misure preventive e protettive di cui all'art. 28 del TUS ed i sistemi di controllo di tali misure;
- elaborare le procedure di sicurezza per le varie attività aziendali;
- proporre i programmi di informazione e formazione dei lavoratori;
- partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro nonché organizzare le riunioni periodiche di prevenzione e protezione dai rischi di cui all'art. 35 del TUS;
- fornire ai lavoratori ogni informazione in tema di tutela della salute e sicurezza sul lavoro che si renda necessaria.

Il medico competente

Il medico competente provvede tra l'altro a:

- collaborare con il Datore di Lavoro e con il RSPP alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della sorveglianza sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori, all'attività di formazione ed informazione nei loro confronti, per la parte di competenza, e all'organizzazione del servizio di primo soccorso considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro;
- programmare ed effettuare la sorveglianza sanitaria;
- istituire, aggiornare e custodire sotto la propria responsabilità una cartella sanitaria e di rischio per ognuno dei lavoratori sottoposto a sorveglianza sanitaria;
- fornire informazioni ai lavoratori sul significato degli accertamenti sanitari a cui sono sottoposti ed informarli sui relativi risultati;
- comunicare per iscritto in occasione della riunione periodica di cui all'art. 35 del TUS i risultati anonimi collettivi della sorveglianza sanitaria effettuata, fornendo indicazioni sul significato di detti risultati ai fini dell'attuazione delle misure per la tutela della salute e della integrità psicofisica dei lavoratori;
- visitare gli ambienti di lavoro almeno una volta all'anno o a cadenza diversa in base alla valutazione di rischi;
- partecipare alla programmazione del controllo dell'esposizione dei lavoratori i cui risultati gli sono forniti con tempestività ai fini della valutazione del rischio e della Sorveglianza Sanitaria.

Il rappresentante dei lavoratori per la sicurezza (RLS)

È il soggetto eletto o designato, in conformità a quanto previsto dagli accordi sindacali in materia, per rappresentare i lavoratori per gli aspetti di salute e sicurezza sui luoghi di lavoro. Riceve, a cura del Datore di Lavoro o di un suo delegato, la prevista formazione specifica in materia di salute e sicurezza.

Appaltatori, fornitori, installatori

In particolare, con riferimento ai terzi:

- gli appaltatori devono: (i) garantire la propria idoneità tecnico-professionale con riferimento ai lavori da eseguire; (ii) recepire le informazioni fornite da Maticmind in merito ai rischi presenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate da Maticmind; (iii) cooperare e coordinare con Maticmind per l'individuazione e l'attuazione delle misure di prevenzione e protezione e degli interventi necessari al fine di prevenire i rischi sul lavoro a cui sono esposti i soggetti coinvolti, anche indirettamente, nell'esecuzione dei lavori da eseguire in appalto o mediante contratto d'opera o di somministrazione;
- i fornitori devono vendere, noleggiare e concedere in uso esclusivamente strumenti ed attrezzature di lavoro, dispositivi di protezione individuali ed impianti che siano conformi alle disposizioni legislative e regolamentari vigenti in materia di salute e sicurezza sul lavoro;

- gli installatori, infine, devono attenersi alle istruzioni fornite dai fabbricanti dei prodotti da installare, con particolare riferimento alle misure e agli adempimenti in materia di salute e sicurezza sul lavoro.

Lavoratori

Per quanto riguarda i lavoratori, ai sensi di quanto previsto dal TUS, ogni individuo deve prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal Datore di Lavoro.

I lavoratori devono in particolare:

- contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;
- osservare le disposizioni e le istruzioni impartite dal Datore di lavoro, dai Dirigenti e dai Preposti, ove nominati, ai fini della protezione collettiva e individuale;
- utilizzare correttamente le attrezzature di lavoro nonché i dispositivi di sicurezza;
- utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;
- segnalare immediatamente al Datore di lavoro, ai Dirigenti o ai Preposti, ove nominati, le deficienze dei mezzi e dei dispositivi di sicurezza nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;
- non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;
- partecipare ai programmi di formazione e di addestramento organizzati dal Datore di Lavoro;
- sottoporsi ai controlli sanitari previsti dal presente decreto legislativo o comunque disposti dal medico competente.

La gestione delle emergenze e primo soccorso

L'organizzazione della gestione delle emergenze e del primo soccorso in Maticmind è parte integrante del Sistema di Gestione Integrato (SGI), in conformità con il D. Lgs. 81/2008 (Testo Unico sulla Sicurezza sul Lavoro) e la norma ISO/IEC 45001:2018. La struttura di gestione è formalizzata attraverso l'Organizzazione della Sicurezza (Safety) e si articola in ruoli, procedure e piani specifici per ciascuna sede aziendale.

La gestione delle emergenze ricade sotto la responsabilità diretta del Datore di Lavoro (DdL) e di figure designate, che devono garantire la pianificazione e l'attuazione delle misure di prevenzione e protezione.

- Datore di Lavoro: ha la responsabilità ultima e poteri gestionali, decisionali e di spesa senza limiti di sorta in materia di SSL e prevenzione incendi. Il DdL provvede a designare preventivamente i lavoratori incaricati delle misure di emergenza (AI e PS);
- Safety & Facility Management / Servizio di Prevenzione e Protezione (RSPP): la funzione Safety supporta il RSPP e le altre strutture aziendali, assicurando il rispetto degli standard di sicurezza e la conformità al D. Lgs. 81/2008 in tutte le sedi, comprese quelle dei Clienti. Il RSPP collabora con il DdL e il Medico Competente nella redazione dei piani di emergenza;
- Preposto alla sicurezza (coordinatore dell'emergenza): questo ruolo è ricoperto tipicamente dal Project Manager (PM) o Area Manager. Il Preposto di sede è il responsabile e coordinatore generale dell'emergenza. I suoi compiti principali includono la direzione e il coordinamento delle operazioni e la ricezione e valutazione dei messaggi.

Per ogni sede sono nominati lavoratori incaricati dell'attuazione delle misure di emergenza:

1. addetti antincendio (AI) / addetti alla gestione delle emergenze;
2. addetti al primo soccorso (PS);
3. addetti alle comunicazioni: assimilabili al preposto/AI, devono allertare il coordinatore e gli enti esterni (112/115/118) in caso di necessità.

La lista completa di questi addetti (AI e PS) è registrata nel Portale SGI.

I processi e le istruzioni operative in caso di emergenza sono dettagliati nel Piano di Gestione delle Emergenze (PGE), che costituisce un allegato specifico al DVR di ciascuna sede. Le emergenze coperte sono:

- emergenza incendio: le procedure dettagliate includono come comportarsi in caso di scoperta di un incendio, come allertare i Vigili del Fuoco e come procedere all'evacuazione;
- primo soccorso: la gestione prevede l'allertamento immediato dell'addetto PS e, in caso di necessità, la chiamata al 118. Le dotazioni sono conservate nelle Cassette di Pronto Soccorso ubicate in luoghi segnalati;
- emergenza sismica: i piani richiedono misure preventive e misure di protezione da attuare durante e dopo la scossa;
- coordinamento esterno (sede di Roma): nel complesso immobiliare di Via Carucci a Roma, dove coesistono più aziende (come Sogei e Maticmind), è attivo un Piano di Emergenza Coordinato (PEC) gestito da un Coordinatore delle Emergenze Esterno (CEE), che è l'operatore alla reception/portineria. Il PEC definisce le interazioni tra i gestori degli edifici (Torre SGR) e i Coordinatori Responsabili delle Emergenze (CRE) interni di ciascuna azienda locataria.

La gestione degli appalti

Nei contratti di appalto o d'opera o di somministrazione devono osservati i principi di seguito indicati ed eventualmente integrati con le procedure aziendali esistenti in materia.

Il Datore di Lavoro, in caso di affidamento di lavori, servizi e forniture all'impresa appaltatrice o a lavoratori autonomi all'interno della propria azienda, e sempre che abbia la disponibilità giuridica dei luoghi in cui si svolge l'appalto o la prestazione di lavoro autonomo, è chiamato a:

- verificare l'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione alle attività da affidare in appalto;
- mettere a disposizione degli appaltatori informazioni dettagliate circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
- coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori, attraverso un costante scambio di informazioni con i datori di lavoro delle imprese appaltatrici anche al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva.

Il Datore di Lavoro committente promuove la cooperazione ed il coordinamento di cui ai punti precedenti elaborando un Documento Unico di Valutazione dei Rischi per le Interferenze nel quale siano indicate le misure adottate per eliminare o, laddove non sia possibile, per ridurre al minimo i rischi da interferenze. Tale documento deve allegarsi al contratto di appalto o d'opera, già in fase di procedura di affidamento, e va adeguato in funzione dell'evoluzione dei lavori, dei servizi e delle forniture.

Le riunioni periodiche di sicurezza

Il datore di lavoro indice almeno annualmente la riunione periodica di cui all'art. 35 TUS per discutere, inter alia:

a) del documento di valutazione dei rischi;

b) dell'andamento degli infortuni e delle malattie professionali e della sorveglianza sanitaria;

c) dei criteri di scelta, le caratteristiche tecniche e l'efficacia dei dispositivi di protezione individuale;

d) dei programmi di informazione e formazione dei dirigenti (ove nominati), dei preposti e dei lavoratori ai fini della sicurezza e della protezione della loro salute.

Viene redatto un apposito verbale, che rimane a disposizione dei partecipanti per la sua consultazione.

3) L'art. 30 lett. d) del D.lgs. 81/2008

L'art. 30 lett. d) del TUS prevede, inoltre, che il Modello deve assicurare che siano adempiuti gli obblighi giuridici con riguardo alle attività di sorveglianza sanitaria.

In particolare, Maticmind, in ossequio alle disposizioni di legge, ha nominato un medico competente per i casi previsti dall'art. 41 (sorveglianza sanitaria) del TUS e a questi sono assegnati i compiti in materia di sorveglianza sanitaria.

In ossequio alle disposizioni di legge, il medico competente:

- collabora alla valutazione dei rischi, alla predisposizione dell'attuazione delle misure, all'attività di informazione e formazione dei lavoratori, per la parte di sua competenza, e all'organizzazione del servizio di primo soccorso (art. 25 c. 1 lett. a) TUS);
- istituisce, aggiorna e custodisce la cartella sanitaria e di rischio dei lavoratori sottoposti a sorveglianza sanitaria (art. 25 c. 1 lett. c) TUS);
- effettua le visite mediche previste dal TUS (art. 41, comma 2 TUS). È oggetto di verifica la circostanza che il Datore di Lavoro e i lavoratori abbiano ricevuto copia scritta del giudizio dal medico competente (art. 41, comma 6-bis TUS);

Il Datore di Lavoro vigila in ogni caso affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità (art. 18 lett. b) TUS).

1) L'art. 30 lett. e) del D.lgs. 81/2001

L'art. 30 lett. e) del TUS prevede, inoltre, che il Modello deve assicurare che siano adempiuti gli obblighi giuridici con riguardo alle attività di informazione e formazione dei lavoratori.

Informazione

L'informazione che Maticmind trasmette ai Destinatari deve essere facilmente comprensibile e deve consentire agli stessi di acquisire la necessaria consapevolezza in merito a:

- le conseguenze derivanti dallo svolgimento della propria attività non conformemente al sistema SSL adottato da Maticmind;
- il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità con la politica aziendale e le procedure e ogni altra prescrizione relativa al sistema di SSL adottato da Maticmind, nonché ai principi indicati nella presente Parte Speciale di loro pertinenza.

Ciò premesso, Maticmind, in considerazione dei diversi ruoli, responsabilità e capacità e dei rischi cui è esposto ciascun lavoratore, fornisce, tra l'altro, adeguata informazione sulle seguenti tematiche:

- rischi specifici dell'impresa, sulle conseguenze di questi e sulle misure di prevenzione e protezione adottate, nonché sulle conseguenze che il mancato rispetto di tali misure può provocare anche ai sensi del Decreto;
- procedure che riguardano il primo soccorso, le misure antincendio, l'evacuazione dei luoghi di lavoro;
- Servizio di Prevenzione e Protezione: nominativi del RSPP e del medico competente.

In merito alle attività di sicurezza che determinano l'aggiornamento del Documento di Valutazione dei Rischi, il RLS viene consultato preventivamente e tempestivamente. Di tutta l'attività di informazione sopra descritta viene data evidenza su base documentale, anche mediante apposita verbalizzazione.

Formazione

Maticmind fornisce adeguata formazione a tutti i lavoratori in materia di sicurezza sul lavoro e il contenuto della stessa, secondo le previsioni del TUS è facilmente comprensibile e consente di acquisire le conoscenze e competenze necessarie.

A tal proposito Maticmind assicura che:

- la formazione sia adeguata ai rischi della mansione cui ognuno dei lavoratori è in concreto assegnato. I lavoratori che cambiano mansione e quelli eventualmente trasferiti ricevono formazione specifica, preventiva e/o aggiuntiva, ove necessario, per il nuovo incarico;
- ognuno dei lavoratori sia sottoposto a tutte quelle azioni formative rese obbligatorie dalla normativa di legge (ad esempio: uso delle attrezzature di lavoro; uso dei dispositivi di protezione individuale; movimentazione manuale di carichi; uso dei videoterminali);
- ogni dirigente ed ogni preposto, se nominati, nonché gli addetti a specifici compiti in materia di emergenza, ricevano un'adeguata e specifica formazione e un aggiornamento periodico in relazione ai propri compiti in materia di SSL;
- siano effettuate periodiche esercitazioni di emergenza di cui deve essere data evidenza (attraverso, ad esempio, la verbalizzazione dell'avvenuta esercitazione con riferimento alle modalità di svolgimento e alle risultanze).

La formazione erogata deve prevedere questionari di valutazione dell'apprendimento. Di tutta l'attività di formazione sopra descritta, deve essere data in ogni caso evidenza su base documentale, anche mediante apposita verbalizzazione.

4) L'art. 30 lett. g) del D.lgs. 81/2008

L'art. 30 lett. g) del TUS prevede, inoltre, che il Modello deve assicurare che siano adempiuti gli obblighi giuridici con riguardo alla acquisizione di documentazioni e certificazioni obbligatorie di legge.

Al fine di contribuire all'implementazione e al costante monitoraggio del sistema adottato per garantire la salute e la sicurezza sul luogo di lavoro, Maticmind assicura che vengano adeguatamente conservati, su supporto informatico o cartaceo, e aggiornati i seguenti documenti:

- la cartella sanitaria, la quale deve essere istituita, aggiornata e custodita dal medico competente;
- il registro degli esposti, da predisporre nell'ipotesi di esposizione ad agenti cancerogeni o mutageni;
- il DVR in cui è indicata la metodologia con la quale si è proceduto alla valutazione dei rischi ed è contenuto il programma delle misure di mantenimento e di miglioramento.

Maticmind è altresì chiamata ad assicurare che:

- RSPP e il medico competente, incaricati dell'attuazione delle misure di emergenza e pronto soccorso, nonché eventuali dirigenti, vengano nominati formalmente;
- venga data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate dal medico competente e, eventualmente, dal RSPP;
- venga conservata la documentazione inerente a regolamenti ed accordi aziendali;

- vengano conservati i manuali e le istruzioni per l'uso di macchine, attrezzature e dispositivi di protezione individuale forniti dai costruttori;
- venga conservata ogni procedura adottata da Maticmind per la gestione della salute e sicurezza sui luoghi di lavoro;
- tutta la documentazione relativa alle attività di cui al precedente paragrafo (Informazione, formazione ed addestramento) venga conservata a cura del RSPP e messa a disposizione dell'OdV.

5) L'art. 30 lett. f) e h) del D.lgs. 81/2008

L'art. 30 lett. f) e h) del TUS prevede, inoltre, che il Modello deve assicurare che siano adempiuti gli obblighi giuridici con riguardo:

- alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure o prassi adottate.

Al fine di garantire l'efficienza del sistema adottato per la gestione della salute e della sicurezza sui luoghi di lavoro, Maticmind:

- assicura un costante monitoraggio delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro;
- assicura un costante monitoraggio dell'adeguatezza e della funzionalità del sistema di gestione della salute e della sicurezza a raggiungere gli obiettivi prefissati e della sua corretta applicazione;
- compie approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere;
- prevede che laddove il monitoraggio abbia ad oggetto aspetti che richiedono competenze specifiche, lo stesso sia affidato a competenti risorse esterne.

B) <u>Adempimenti in materia di gestione ambientale</u>

La gestione ambientale in Maticmind è parte del Sistema di Gestione Integrato (SGI) e si basa su un impegno strategico verso la sostenibilità, supportato da certificazioni internazionali, politiche aziendali e procedure operative specifiche.

Maticmind ha infatti ottenuto certificazioni specifiche per la sostenibilità ambientale, quali:

- UNI EN ISO 14001:2015 (Sistemi di Gestione Ambientale - SGA): questo standard fornisce i requisiti per l'identificazione, la valutazione e la gestione degli aspetti ambientali significativi legati alle attività dell'organizzazione;
- UNI EN ISO 14064-1:2019 (Gas a Effetto Serra - GHG): questa certificazione riguarda la quantificazione e la rendicontazione delle emissioni di gas ad effetto serra (GHG) e supporta l'attuazione di politiche di carbon management.

L'applicazione di queste certificazioni ambientali mira, tra l'altro, a ridurre sprechi e consumi energetici e a gestire la produzione e lo smaltimento dei rifiuti.

La Direzione Compliance, Sustainability, Risk Management & Safety è incaricata di monitorare la conformità alle Norme ISO, nonché di definire e sviluppare i piani ESG e CSR (Responsabilità Sociale d'Impresa), con l'impegno di promuovere un'economia sostenibile e a garantire che la Società operi con accuratezza e trasparenza anche in ambito ambientale.

Inoltre, Maticmind si impegna a estendere i principi di sostenibilità lungo la catena dei fornitori, anche tramite attività mirate di due diligence.

Gestione operativa degli aspetti ambientali

La gestione operativa si concentra principalmente sulla minimizzazione degli impatti ambientali derivanti dalle attività tipiche di un system integrator (uffici, logistica e servizi), e in particolare:

- Gestione dei rifiuti e materiali: i processi aziendali comprendono la gestione del rischio di reati ambientali legati alla gestione dei rifiuti, attraverso:
  - procedure di smaltimento: per la prevenzione dei reati ambientali, Maticmind deve ingaggiare periodicamente un fornitore qualificato per lo smaltimento del materiale hardware destinato alla rottamazione. Il fornitore è tenuto a rilasciare la documentazione che attesta il ritiro e il rituale smaltimento;
  - obblighi del magazzino: la funzione Logistica è responsabile della gestione dei rifiuti (imballaggi e/o apparati obsoleti) a norma di legge, mediante accordi quadro con aziende specializzate.
- Monitoraggio delle emissioni e mobilità: la Società ha adottato procedure per monitorare e gestire le emissioni legate alle proprie attività:
  - la procedura SGA_Calcolo Emissioni GHG per la quantificazione e la rendicontazione delle emissioni di gas a effetto serra, funzionale alla gestione dell'inventario GHG;
  - la procedura Gestione Mobility Management Mobilità (PA810_3) per la gestione della mobilità aziendale, che copre gli spostamenti del personale in itinere, monitorando il traffico veicolare indotto.

9 SEZIONE 9: GESTIONE DELLE RISORSE UMANE

PROCESSI	ATTIVITÀ SENSIBILI	FUNZIONE COINVOLTA	REATI PRESUPPOSTO RILEVANTI
Selezione e assunzione del personale	- Gestione del processo di selezione del personale, inclusa la raccolta delle candidature e il reclutamento dei candidati - Stipula, modifica, rinnovo dei contratti di lavoro - Definizione della politica retributiva del personale	- RU - DIR - Datore di Lavoro - Studio Paghe - Marketing - Amministrazione	- Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24) - Delitti di criminalità organizzata (art. 24 ter) e reati transnazionali (L. 146/2006) - Corruzione e traffico di influenze illecite (art. 25) - Reati societari (art. 25 ter) - Intermediazione illecita e sfruttamento del lavor (art. 25 quinquies) - Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 septies) - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio (art. 25 octies) - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies) - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 duodecies)
Gestione amministrativa e contabile del personale	- Definizione degli obiettivi e valutazione delle performance del personale - Formulazione delle proposte di avanzamento di carriera e/o dei corrispettivi variabili - Gestione del processo di salary.review - Rilevazione di presenze, straordinari, permessi e ferie del personale dipendente - Elaborazione degli stipendi e/o dei compensi e tutte le spettanze da liquidare ai dipendenti - Calcolo dei contributi e trattenute fiscali inerenti i corrispettivi - Gestione dei benefit. aziendali - Gestione trasferte, anticipi, rimborsi spese - Spese di rappresentanza		

Formazione del personale	- Monitoraggio e gestione delle attività di formazione e aggiornamento		- Reati tributari (art. 25 quinquiesdecies)

9.1 Alcuni esempi dei Reati Presupposto rilevanti nella Gestione delle Risorse Umane

Si riportano qui di seguito, a titolo esemplificativo, alcune delle potenziali condotte penalmente rilevanti in relazione alle Aree di rischio sopra menzionate:

a) Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24)

   - viene simulato illecitamente lo svolgimento di formazione finanziata in favore dei dipendenti della Società, al fine di ottenere finanziamenti non dovuti.

b) Corruzione e traffico di influenze illecite (art. 25)

   - tra i vari candidati per una posizione lavorativa all'interno della Società, viene selezionato in maniera impropria o arbitraria/soggettiva un candidato vicino o collegato a soggetti pubblici o a loro intermediari, al fine di ottenere un indebito vantaggio per la Società.

c) Delitti contro la libertà individuale (art. 25 quinquies)

   - la Società stipula un contratto di somministrazione di manodopera con un'agenzia interinale che adotta garanzie, tutele e retribuzione inferiori a quanto previsto dai Contratti Collettivi di settore.

d) Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 septies)

   - un lavoratore appena assunto, non adeguatamente formato sui rischi specifici della mansione o dell'ambiente di lavoro, subisce (o causa) un infortunio.

e) Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 duodecies)

   - vengono assunti lavoratori stranieri privi del permesso di soggiorno, o il cui permesso sia scaduto (e del quale non sia stato richiesto nei termini di legge il rinnovo), revocato o annullato.

9.2 Le regole generali di condotta nella Gestione delle Risorse Umane

I Destinatari della presente Parte Speciale devono:

- rispettare rigorosamente la normativa vigente in materia di lavoro, previdenza, sicurezza sul lavoro, immigrazione, pari opportunità, lavoro minorile, privacy e trattamento dei dati personali, nonché i contratti collettivi nazionali applicabili, il Codice Etico e le policy aziendali in ambito HR;
- adottare criteri oggettivi, trasparenti e documentabili nei processi di selezione e assunzione del personale, assicurando la parità di trattamento e l'assenza di discriminazioni di qualsiasi natura;

- operare nel rispetto del principio di imparzialità, evitando favoritismi, conflitti di interesse, pressioni esterne o pratiche che possano compromettere la correttezza delle decisioni di assunzione e di gestione;
- tutelare la riservatezza delle informazioni e dei dati personali acquisiti in qualunque fase del rapporto di lavoro, nel rispetto delle normative vigenti in materia di protezione dei dati;
- garantire la corretta gestione amministrativa e contabile del personale, assicurando che ogni operazione sia giustificata, documentata, tracciabile e coerente con gli obblighi contrattuali e normativi;
- astenersi da qualsiasi condotta che possa generare falsificazioni, omissioni o irregolarità nella registrazione delle presenze, nella gestione delle retribuzioni o nei flussi contributivi;
- promuovere e sostenere lo sviluppo delle competenze del personale, assicurando che le attività formative siano coerenti con i fabbisogni aziendali, trasparenti nella selezione dei partecipanti e correttamente documentate;
- utilizzare le risorse destinate alla formazione in modo efficace, efficiente e conforme alle finalità previste, evitando sprechi o usi impropri di fondi pubblici o privati eventualmente destinati a tale scopo;
- adottare un comportamento improntato a correttezza, responsabilità e professionalità in tutte le fasi del rapporto di lavoro, contribuendo alla costruzione di un ambiente di lavoro rispettoso, inclusivo e collaborativo;
- ripudiare qualsiasi forma di sfruttamento del personale e violazione dei diritti individuali e contrattuali dei propri dipendenti e collaboratori, nonché di soggetti terzi operanti con la stessa;
- creare un ambiente di lavoro che garantisca condizioni rispettose della dignità personale e nel quale le caratteristiche dei singoli non possano dare luogo a discriminazioni o condizionamenti;
- astenersi dall'instaurare rapporti con soggetti sui quali incombe il sospetto di operare nell'orbita di associazioni o gruppi criminosi, o con soggetti che si mostrino reticenti nel fornire tutte le informazioni necessarie ai fini di una trasparente conoscenza del loro passato professionale;
- collaborare attivamente con gli organi di controllo interni e/o esterni, fornendo informazioni veritiere e complete, e segnalando tempestivamente eventuali anomalie, criticità o violazioni rilevate nell'ambito delle attività HR.

9.3 I protocolli di condotta specifici

Struttura e Responsabilità

La funzione HR (RU) elabora le politiche del personale in accordo con la Direzione Aziendale (DIR) e ne assicura l'applicazione. Le principali aree di attività coprono: la selezione, l'inserimento, l'amministrazione, la formazione, la fidelizzazione e il performance management.

Reclutamento e onboarding

Le seguenti attività rientrano nell'ambito della gestione del personale e mirano a garantire che la Società disponga delle competenze necessarie, in un'ottica di trasparenza, indipendenza e meritocrazia:

Attività	Dettaglio del Processo	Procedure/Documenti Chiave
Individuazione Fabbisogno	DIR, supportata dai Responsabili di funzione e da RU, valuta la reale necessità di aumentare l'organico, la capacità economica di nuove assunzioni e il massimo impegno economico (budget). Vengono definite le caratteristiche professionali richieste ("Job Title" e "Job Description").	Modulo destinato alla "Selezione del Personale" dell'applicativo Zucchetti.
Ricerca (Recruiting)	La ricerca può essere interna (tramite job posting) o esterna (tramite autocandidature, servizi di placement, inserzioni sul sito web o agenzie specializzate). RU coordina la ricerca.	
Selezione e Screening	Vengono eseguiti uno screening preliminare dei CV e interviste. L'esito del colloquio è tracciato da RU nella Scheda valutazione colloquio e nel tool Zucchetti. In caso di esito positivo, RU sottopone la proposta di assunzione che definisce gli aspetti contrattuali ed economici (ruolo, inquadramento, benefit).	Scheda valutazione colloquio
Assunzione	RU predispone il contratto di lavoro firmato da DIR e dall'interessato. Il candidato deve fornire documenti come copia del permesso di soggiorno valido (per lavoratori stranieri non UE) e il modulo anti-pantouflage, per dichiarare l'assenza di conflitti di interesse con la Pubblica Amministrazione. RU invia la Comunicazione Obbligatoria (UNILAV) al Centro per l'Impiego e lo Studio di Consulenza del Lavoro esterno.	Contratto di lavoro, modulo anti-pantouflage
Onboarding e Inserimento	RU consegna il Welcome Kit, che include la Dichiarazione di presa visione del Codice Etico e del Modello, il Codice Disciplinare e le informative sulla Privacy. Vengono fornite le dotazioni personali (badge, PC, cellulare) e create le utenze di accesso ai sistemi interni (SIM, Navision, Zucchetti).	Welcome Kit

Amministrazione del personale e gestione spese

RU provvede mensilmente, secondo scadenze concordate con lo Studio Paghe, all'invio di dati per l'elaborazione dei cedolini del personale dipendente e non dipendente.

Questi dati provengono dal dipendente:

- via mail, fornendo specifici moduli o altra documentazione;
- tramite l'utilizzo degli applicativi del sistema Zucchetti;
- da altre fonti interne ed esterne all'azienda (ad esempio, mail della Direzione RU nel caso di promozioni e aumenti).

Oltre alle variabili legate alle presenze, prima dell'invio allo Studio Paghe, RU gestisce e controlla altri tipi di variabili (trattenute e diarie, cambiamenti di centro di costo, numero di buoni pasto spettanti, TFR).

In seguito al passaggio delle suddette variabili da parte di RU, lo Studio Paghe si occupa dell'elaborazione dei cedolini, sottoposti ad un controllo finale da parte di RU prima della chiusura della fase di elaborazione paghe, della pubblicazione del cedolino finale in Zucchetti, del passaggio dei netti dello stipendio all'Amministrazione, incaricata della trasmissione dei bonifici.

Oggetto del controllo dei cedolini sono i dati relativi alle variabili trasmesse allo Studio Paghe, affinché siano state correttamente recepite ed elaborate le informazioni.

RU controlla mensilmente le note spese compilate dal personale mediante il modulo ZTravel di Zucchetti.

La maggior parte dei controlli sono automatizzati e conseguentemente il livellamento delle eccedenze rispetto agli importi dei massimali previsti è effettuato direttamente dal modulo ZTravel.

Il controllo da parte di RU consiste principalmente nella verifica della presenza di scontrini corrispondenti all'importo inserito, dell'importo dei servizi di viaggio, nel confronto degli importi delle spese sostenute con carta di credito aziendali rispetto all'estratto conto mensile delle carte di credito fornito dalla funzione Amministrazione.

Con riferimento alla gestione delle spese di rappresentanza, si veda il relativo paragrafo sub 3.3.

Formazione del personale e relativi costi

La formazione si divide in due tipologie principali, con diverse modalità di gestione:

Tipologia di Formazione	Dettaglio del processo	Gestione dei costi
Formazione Tecnica	È finalizzata ad incrementare le competenze tecnologiche (certificazioni, aggiornamenti) ed è affidata alla responsabilità del Marketing (MRKT).	I piani sono proposti dal responsabile di funzione in fase di budget e approvati da DIR. Per assicurare la tracciabilità e la linearità del processo, i corsi e le

Formazione Trasversale	Riguarda l'aderenza a normative cogenti (D. Lgs. 81/2008; D. Lgs. 231/2001; GDPR). È gestita da RU in collaborazione con il Datore di Lavoro, per quanto la sicurezza. Include la formazione base e specifica per tutti i dipendenti, erogata con piattaforma online e soggetta ad aggiornamento ogni 5 anni.	certificazioni sono pagati dalla Società, che richiede in un secondo momento il rimborso a ciascun partecipante.

Lavoro interinale e distacco

Maticmind utilizza personale esterno in regime di distacco o somministrazione (staff leasing):

- somministrazione (staff leasing): la risorsa è assunta direttamente da un'agenzia (società somministratrice), che rimane il Datore di Lavoro responsabile degli adempimenti retributivi e contributivi. Maticmind è l'azienda utilizzatrice e RU gestisce gli aspetti organizzativi (badge, utenze);
- distacco/subappalto: quando il personale di fornitori terzi opera presso Maticmind o i suoi Clienti in regime di distacco, RU supporta il Project/Service Manager, richiedendo al fornitore la documentazione necessaria per il perfezionamento delle posizioni, inclusi documenti di identità e permesso di soggiorno per i lavoratori stranieri. Tale documentazione è gestita nell'Albo Fornitori, con massima attenzione per la verifica delle capacità professionali del fornitore in caso di distacco.

Sistema disciplinare e controlli

Il sistema disciplinare ha una funzione essenziale per l'efficacia del Modello, in quanto sanziona la mancata osservanza delle procedure interne. Il sistema adottato da Maticmind fa infatti riferimento al Codice Disciplinare aziendale, al CCNL applicato e al Modello.

Le violazioni del Codice Etico e del Modello sono considerate illeciti disciplinari e possono portare a sanzioni progressive che, nei casi più gravi, includono il licenziamento senza preavviso.

Con riferimento ai controlli, Maticmind monitora le risorse IT in dotazione ai dipendenti (come i PC) tramite controlli di tipo difensivo (come quelli condotti dal SOC - Security Operation Center) per prevenire illeciti. Tale controllo è effettuato nel rispetto dell'art. 4 dello Statuto dei Lavoratori e del GDPR, bilanciando la tutela del patrimonio aziendale con il diritto alla riservatezza del dipendente. I controlli procedono in modo graduale, partendo da verifiche su dati aggregati per poi passare a ispezioni individuali solo in caso di persistenza di anomalie.

9.4 Le procedure specifiche

Al fine di prevenire o ridurre al minimo il rischio di commissione delle fattispecie di reato rilevanti nello svolgimento delle attività sensibili, la Società ha adottato delle procedure specifiche che disciplinano

l'intero ciclo di attività HR, dalla selezione del personale alla sua gestione amministrativa, inclusi gli aspetti di conformità e sicurezza. Tali procedure, a cui si fa integralmente rinvio, costituiscono parte integrante del presente Modello.

Di seguito sono elencate le procedure applicabili in materia di gestione delle risorse umane:

1. Procedure centrali di gestione del personale

- Gestione delle risorse umane (PAQ712_1): tale procedura descrive le attività principali relative alla gestione delle risorse umane, che includono la selezione del personale, l'inserimento in azienda, la gestione e amministrazione, la pianificazione dei percorsi formativi, la gestione della formazione, la fidelizzazione del personale e il performance management. In particolare, la procedura riguarda le seguenti aree di responsabilità:
  - selezione e assunzione: guida il processo di assunzione di nuove risorse, in coordinamento con i responsabili di funzione;
  - gestione amministrativa: governa il processo di payroll e assicura la corretta applicazione della normativa giuslavoristica;
  - compliance: coordina la formazione in ambito salute e sicurezza (D.Lgs. 81/2008), compliance relativa al D.Lgs. 231/2001 e privacy (GDPR);
  - gestione dei terzi: riguarda la gestione del personale di fornitori e terze parti in regime di distacco.

2. Procedure amministrative e finanziarie

- Manuale Operativo Ztravel: la Società ha implementato due manuali operativi specifici che supportano la gestione delle spese:
  - Manuale Operativo Ztravel_Gestione Trasferte;
  - Manuale Operativo Ztravel_Gestione Note Spese.

  I Manuali Operativi Ztravel descrivono la pianificazione e l'amministrazione delle trasferte, inclusi l'inserimento delle richieste, la prenotazione dei servizi di viaggio e la successiva rendicontazione delle note spese da parte dei dipendenti, con il controllo dei massimali di spesa e l'approvazione dei responsabili.

3. Procedure di compliance, etica e sicurezza

- Procedura di gestione dei regali, viaggi e sponsorizzazioni (PAQ820_4): stabilisce le regole di condotta per i dipendenti, i dirigenti, i collaboratori e i consulenti della Società riguardo alla ricezione e all'offerta di regali e viaggi, con l'obiettivo di prevenire atti di corruzione.
- Disciplinare sulla sicurezza delle informazioni (SGSI_G005): definisce le regole per l'utilizzo delle risorse IT aziendali (hardware, software, credenziali) da parte degli utenti, vietando l'uso

improprio e definendo il comportamento professionale atteso, con applicabilità a ogni dipendente e collaboratore.

- Procedura gestione nomine AdS (GDPR_PR001): documenta il processo di gestione delle nomine ad Amministratore di Sistema (AdS). RU ha la responsabilità di verificare e decidere formalmente le nomine AdS per il personale interno, inoltrarle al titolare per la firma e registrarle.
- Sistema di Gestione Integrato e certificazioni, con particolare riferimento alle seguenti certificazioni:
  - ISO/IEC 45001:2018 (Salute e Sicurezza sul Lavoro - SGSSL);
  - UNI-ISO 37001:2016 (Anti-Bribery Management System);
  - UNI/PdR 125:2022 (Parità di Genere).

4. Procedure relative al rapporto con terze parti (appalti e distacchi)

- Gestione sicurezza negli appalti (PAQ812_1): questa procedura è rilevante per la funzione RU quando riguarda l'impiego di personale di fornitori esterni in regime di distacco. La funzione RU supporta infatti i Project/Service Manager richiedendo ai fornitori la documentazione necessaria per il perfezionamento delle posizioni del personale distaccato, gestendo tale documentazione nell'Albo Fornitori.