P&P Technology srl

MODELLO ORGANIZZATIVO - PARTE SPECIALE – Rev 01
AI SENSI DEL D.LGS. 231/2001 PER MICRO E PICCOLE IMPRESE
Aggiornato al 02/12/2025

Approvato da: Andrea Perpignani, Amministratore Unico____	Data: 02/12/2025

Data revisione :

Introduzione

Il presente documento costituisce la Parte Speciale del Modello Organizzativo adottato da P&P Technology srl, microimpresa operante nel settore Formazione del personale, ai sensi del D.Lgs. 231/2001.

Modifiche rispetto alla versione precedente

Le modifiche sono state eseguite a seguito dell'analisi dei rischi aggiornata al 20/11/2025 e considerando le richieste di integrazione della Regione Lombardia del 18/11/2025

Premessa e Finalità

Il presente Modello di Organizzazione, Gestione e Controllo (MOG), redatto ai sensi del D.Lgs. 231/2001, è adottato nella forma semplificata prevista per le microimprese. L'obiettivo è prevenire la commissione dei reati rilevanti per la responsabilità amministrativa degli enti, mediante un sistema organizzativo proporzionato alle dimensioni e alla natura dell'azienda.

Struttura della Società

- Denominazione azienda: P&P Technology srl
- Settore di attività: Formazione del personale
- Struttura organizzativa: Microimpresa senza rapporti con la Pubblica Amministrazione e senza impatti ambientali
- Principali processi aziendali: Progettazione, realizzazione ed erogazione di contenuti formativi esclusivamente per le aziende, sia in modalità in presenza che in e-learning (sincrono e asincrono)
- Numero dipendenti: 2

Codice Etico e Regole di Comportamento

L'azienda adotta un Codice Etico che definisce principi di integrità, trasparenza, legalità, riservatezza dei dati e correttezza nei rapporti con clienti, fornitori e collaboratori.

Sistema Disciplinare: reati e sanzioni

Come viene riportato nel Codice Etico approvato da codesta società, di seguito vengono riportate le sanzioni definite nel Codice Disciplinare aziendale, che richiamano il CCNL Commercio e le norme di legge, come il Codice Civile (art. 2104, 2105, 2106). Le sanzioni sono applicate dal **Datore di Lavoro** (o suoi delegati, come i dirigenti/responsabili) seguendo una procedura ben precisa, prevista dalla legge (Art. 7 Statuto dei Lavoratori) e dal **CCNL** (Commercio, Terziario), che richiede la contestazione scritta dell'addebito e la possibilità per il lavoratore di presentare difese prima dell'irrogazione.

Principi Chiave:

- **Gradualità**: La sanzione deve essere proporzionata alla gravità dell'infrazione.
- **Procedura**: Per multe e sospensioni è prevista una procedura (contestazione scritta, termine per difesa del lavoratore).
- **Progressione**: Le sanzioni aumentano con la gravità e la recidiva, ma le sanzioni più lievi decadono dopo due anni.

Tipologia di Sanzioni (in ordine crescente di gravità):

1. **Richiamo Verbale** (o Ammonizione): Per mancanze più lievi, come lievi ritardi o negligenze.
2. **Richiamo Scritto**: Per recidiva o mancanze più significative.
3. **Multa**: Ritenuta sulla retribuzione, non superiore a 4 ore della normale retribuzione, per mancanze come ritardi, negligenza o assenze ingiustificate brevi,
4. **Sospensione dal Servizio e dalla Retribuzione**: Per fatti particolarmente gravi, non superiore a 10 giorni, come gravi infrazioni alla sicurezza sul lavoro, reati in materia di violazione dei diritti di autore reati Ambientali, reati in materia di Whistleblowing, concorrenza sleale, reati in materia di Privacy- GDPR.
5. **Risoluzione del contratto di lavoro**: Per comportamenti recidivi o talmente gravi da non consentire la prosecuzione del rapporto (es.). reati contro la Pubblica Amministrazione, reati Societari, reati sicurezza sul lavoro, per violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, furto, abuso d'ufficio, insubordinazione grave, concorrenza sleale, ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, reati Tributari, reati in materia di Privacy- GDPR- Accesso abusivo ai sistemi informativi-databreach

Ambiti di rischio e attività sensibili

L'analisi dei rischi ha identificato le seguenti aree di attività sensibili in relazione ai reati previsti dal D.Lgs. 231/2001:

- Reati contro la Pubblica Amministrazione
- Reati Societari
- Reati sicurezza sul lavoro, per violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita
- Reati in materia di violazione dei diritti di autore
- Reati Ambientali
- Reati Tributari
- Reati in materia di Privacy- GDPR- Accesso abusivo ai sistemi informativi-databreach
- Reati in materia di Whistleblowing
- Negligenze, ritardi sull'orario di lavoro, ritardi sull'avvio delle attività di formazione

All'interno del documento di Analisi dei rischi, vengono presentati e spiegati i reati non Vengono inoltre presenti i reati non applicabili.

Protocolli di Controllo

Vengono presentate le principali misure preventive, maggiori dettagli vengono presentati negli allegati specifici dei reati previsti.

- Tracciabilità dei flussi finanziari, completa di pagamenti e incassi
- Controllo amministrativo esterno qualificato
- Gestione sicura dei dati e sistemi informatici
- Verifica dei fornitori e dei contratti
- Monitoraggio delle operazioni commerciali e amministrative.
- Politiche di sicurezza sul lavoro e formazione obbligatoria.
- Monitoraggio periodico degli accessi alla piattaforma on-line
- Adozione di sistemi di protezione dati e sicurezza informatica.
- Procedure per la segnalazione di irregolarità
- Riservatezza e protezione dei dati dei clienti
- Conservazione ordinata dei documenti
- Formazione interna periodica su privacy e sicurezza informatica

Organismo di Vigilanza (OdV)

L'azienda adotta un OdV monocratico, dotato di requisiti di autonomia, indipendenza e professionalità. L'OdV vigila sul funzionamento e sull'efficacia del Modello e propone aggiornamenti quando necessario.

Flussi Informativi verso l'OdV

L'azienda garantisce i seguenti flussi informativi per tutte le classi di reato previste verso l'OdV:

- eventuali segnalazioni interne di comportamenti non conformi
- anomalie amministrativo-contabili
- aggiornamenti societari o variazioni organizzative
- report periodici sulla gestione della privacy

Si allega al presente documento i Flussi informativi.

Sistema Whistleblowing

È istituito un canale di segnalazione riservato e protetto, conforme al D.Lgs. 24/2023, proporzionato alle dimensioni della microimpresa. Le segnalazioni sono ricevute direttamente dall'OdV, tramite l'indirizzo odv.pandp@gmail.com

Selezione Fornitori e Collaboratori

Obiettivo: Garantire trasparenza e correttezza nella scelta di fornitori e collaboratori.

Procedure:

- Definizione di criteri oggettivi e verificabili per la selezione.
- Controllo della conformità legale e fiscale dei fornitori.
- Monitoraggio della qualità delle prestazioni fornite.
- Registrazione e archiviazione dei contratti e delle comunicazioni con i fornitori.

Misure di prevenzione:

- Liste di fornitori qualificati basate su valutazioni periodiche.
- Clausole nei contratti che vietano pratiche illecite o comportamenti scorretti.
- Procedure per la segnalazione di irregolarità.
- Attinenza alle procedure stabilite da certificato di qualità EA37

La società ha adottato una valutazione annuale dei Fornitori al fine di garantire il mantenimento qualitativo degli stessi. Laddove non venisse rispettato lo standard richiesto, la società cesserà qualsiasi rapporto con gli stessi.

Formazione e Aggiornamento del Modello

Il Modello è accompagnato da un'attività formativa minima rivolta ai soggetti apicali e operativi.
L'aggiornamento avviene annualmente o a seguito di modifiche normative o organizzative.

Piano di Formazione Interna

Obiettivo: Sensibilizzare dipendenti e collaboratori sui principi del Modello 231 e sulle responsabilità connesse.

Metodi:

- Corsi online con test di verifica.
- Sessioni formative in presenza con esperti del settore, dove richiesto
- Distribuzione di manuali e materiale informativo.
- Simulazioni di casi pratici per migliorare la comprensione dei rischi aziendali, dove richiesto

Destinatari:

- Dipendenti della Società.
- Obbligo di adesione alle informative presenti nella pagina Trasparenza e Compliance del sito Web, per tutti coloro che operano con la Società.

Frequenza:

- Formazione iniziale obbligatoria per i nuovi ingressi.
- Aggiornamenti periodici almeno una volta all'anno.
- Incontri straordinari in caso di modifiche normative o aziendali rilevanti.

Monitoraggio e valutazione:

- Questionari di apprendimento per verificare la comprensione dei concetti chiave.
- Report periodici sugli esiti della formazione e sul livello di conformità aziendale.
- Eventuali azioni correttive in caso di carenze individuate.

Alleghiamo, materiale informativo interno distribuito ai collaboratori, registri formazione obbligatoria

Attuazione e Monitoraggio

L'amministratore garantisce l'efficace attuazione del Modello e ne assicura l'aggiornamento periodico in funzione dell'evoluzione normativa.

Allegati

Al presente documento vengono allegati i seguenti dettagli

Flussi Informativi verso OdV

Milano, 02/12/2025	**FLUSSI INFORMATIVI** ***VERSO L'ORGANISMO DI VIGILANZA*** **MODELLO ex D.Lgs. 231/01**	Vers. 1.0

REATO	FLUSSI	FREQUENZA	AD EVENTO
1 - Reati contro la Pubblica Amministrazione Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (Art. 24, D.Lgs. n. 231/2001) [articolo modificato dalla L. 161/2017, dal D.Lgs. n. 75/2020 e dalla L. n. 137/2023] Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità e corruzione (Art. 25, D.Lgs. n. 231/2001) [modificato dalla L. n. 190/2012, dalla L. 3/2019, dal D.Lgs. n. 75/2020, dalla L. 112/2024 e dalla L. 114/2024]	▪ Provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità dai quali si evinca lo svolgimento delle indagini, anche nei confronti di ignoti per i reati di cui al D.lgs. 231/2001;		X
	▪ Comunicazioni interne ed esterne riguardanti qualsiasi fattispecie che possa essere messa in collegamento con ipotesi di reato di cui al D.Lgs. 231/01 (ad es. provvedimenti disciplinari avviati/attuati a tale titolo nei confronti dei dipendenti);		X
	▪ Notizie relative a cambiamenti organizzativi;	Semestrale	
	▪ Aggiornamenti del sistema delle deleghe;	Semestrale	
	▪ Comunicazioni riguardanti carenze nel sistema di controllo interno o fatti censurabili;		X
	▪ Rapporti contrattuali intrattenuti con la Pubblica amministrazione;		X
	▪ Erogazioni pubbliche.		X
	• Ispezioni da parte di organi esterni preposti al controllo (Inail, Inps, Agenzia delle Entrate, Enti finanziatori, ecc.)		X

	• Verifiche di terze parti, sistema di qualità ed altri soggetti	Semestrali	
2 - Reati societari (Art. 25-ter, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 61/2002, modificato dalla L. n. 190/2012, dalla L. 69/2015, dal D.Lgs. n.38/2017 e dal D.Lgs. n. 19/2023]	Comunicazione da parte di soggetti preposti al controllo, sia interni Revisore, sia esterni (esempio Agenzia delle Entrate),		X
3 - 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, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 123/2007; modificato L. n. 3/2018]	Comunicazioni da parte del datore di lavoro e da parte dell'RSPP relative all'ordinaria attività di mantenimento per la gestione della salute e sicurezza del lavoro	Semestrale	
	Infortuni sul lavoro o in itinere		X
	Comunicazione da parte di soggetti preposti al controllo, esterni (ATS)		X
4 - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonchè autoriciclaggio (Art. 25-octies, D.Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 231/2007; modificato dalla L. n. 186/2014 e dal D.Lgs. n. 195/2021]	Comunicazione da parte di soggetti preposti al controllo, esterni.		
5 - Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) Articolo aggiunto dalla L. n. 99/2009; modificato dalla L. n. 93/2023 e dalla L. n. 166/2024]	Comunicazione da parte di soggetti preposti al controllo, esterni (SIAE, Fornitori di contenuti digitali)		X
6 - Reati ambientali (Art. 25-undecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 121/2011, modificato dalla L. n. 68/2015, modificato dal D.Lgs. n. 21/2018 e modificato dalla L. n. 137/2023]	Registrazione del conferimento di rifiuti diversi dagli urbani o non assimilabili	Semestrale	

7 - Reati Tributari (Art. 25-quinquesdecies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 157/2019 e dal D.Lgs. n. 75/2020]	Comunicazione da parte di soggetti preposti al controllo, sia interni Revisore, sia esterni (Agenzia delle Entrate)		X
8 - Delitti informatici e trattamento illecito di dati (Art. 24-bis, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008; modificato dal D.Lgs. n. 7 e 8/2016 e dal D.L. n. 105/2019]	Incidente sulla sicurezza dei dati che può aver compromesso integrità, riservatezza o disponibilità degli stessi. Segnalazioni di terze parti di un evento critico, segnalazioni del DPO		X
9 - Reati in materia di Whistleblowing	Altre segnalazioni di Whistleblowing fuori dal canale previsto.		X

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO PREDISPOSTO AI SENSI DEL D.LGS 231/2001

PARTE SPECIALE - 1

REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

STATO DI REVISIONE DEL DOCUMENTO

Approvato da: Andrea Perpignani, Amministratore Unico____	Data: 02/12/2025

Data revisione :

Descrizione del documento

Ai sensi dell'art. 6 comma 2, lett. a) del D.Lvo 231/01, P&P Technology srl, attraverso un processo di mappatura dei rischi, di valutazione delle attività, dei controlli esistenti e del contesto aziendale in cui opera (cd. *control and risk self assessment)*, ha identificato i processi e le attività *sensibili* nell'ambito delle quali possano essere potenzialmente commessi i reati contro la Pubblica Amministrazione previsti dal D.Lvo 231/2001.

Per il contrasto al rischio di commissione di tali reati si richiama quanto disposto dal Modello Organizzativo Parte Generale approvato da P&P Technology srl, e tutti i destinatari del Modello sono tenuti ad adottare regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento ed ai principi contenuti nel Codice Etico.

I principi individuati nel Codice Etico, che qui viene integralmente richiamato costituiscono presupposto e parte integrante dei presidi e delle Misure di controllo descritte nella presente Parte Speciale con riferimento alle diverse tipologie di destinatari e/o *stakeholders*, nell'ambito delle diverse aree di rischio individuate.

La presente Parte Speciale potrà essere aggiornata dal Presidente o dalla Direzione e tale aggiornamento sarà sottoposto a validazione da parte dell'OdV.

REATO PRESUPPOSTO: (art. 24 D.Lgs. 231/01).

Reati commessi nei rapporti con la Pubblica Amministrazione

- *Corruzione per un atto d'ufficio (art. 318 c.p.);*
- *Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.);*
- *Corruzione in atti giudiziari (art. 319-ter c.p.);*
- *Istigazione alla corruzione (art. 322 c.p.);*

Premessa

Sulla base delle analisi condotte sono considerati applicabili a P&P Technology srl i seguenti reati nei rapporti con la Pubblica Amministrazione:

corruzione per l'esercizio della funzione, costituito dalla condotta del pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa;

corruzione per un atto contrario ai doveri d'ufficio, costituito dalla condotta del pubblico ufficiale il quale, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altre utilità, o ne accetta la promessa;

induzione indebita a dare o promettere utilità, costituito dalla condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, salvo che il fatto costituisca più grave reato, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità, nonché dalla condotta di colui che dà o promette il denaro o altra utilità;

istigazione alla corruzione, costituito dalla condotta di chi offre o promette denaro od altre utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio per l'esercizio delle sue funzioni o dei suoi poteri, o per indurre lo stesso a omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, qualora l'offerta o la promessa non sia accettata, nonché dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri o che sollecita una promessa o dazione di denaro od altre utilità da parte di un privato per le finalità indicate dall'art. 319 c.p.;

Processi Aziendali

I reati suddetti e le attività sensibili indicate di seguito impattano sui seguenti processi aziendali:

- Amministrazione, Controllo, Pianificazione;
- Gare d'appalto / bandi di gara e Contratti P.A.
- Relazioni Esterne
- Erogazione dei servizi

Attività Sensibili

La Società ha individuato le seguenti Attività Sensibili e strumentali, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i citati reati nei rapporti con la P.A. previsti dal Decreto:

I. Gestione del processo di acquisto di beni e servizi (inclusa selezione, qualifica e gestione fornitori);
II. Assegnazione di consulenze e di prestazioni professionali;
III. Gestione delle attività e degli adempimenti connessi alla fiscalità;
IV. Gestione delle risorse finanziarie (incassi e pagamenti);
V. Gestione delle spese di rappresentanza;
VI. Selezione ed assunzione del personale;
VII. Operazioni di sponsorizzazione ed erogazioni liberali;
VIII. Gestione dei rapporti con i rappresentanti della PA in occasione di accertamenti, ispezioni, verifiche.

Procedure e Misure di prevenzione

I. *Operazioni riguardanti la **gestione del processo di acquisto** di beni e servizi (inclusa selezione, qualifica e gestione fornitori). I protocolli prevedono che:*

- l'intero iter di valutazione e selezione dei fornitori, ivi compresi quelli per la realizzazione di investimenti tecnici, sia strutturato secondo i principi di trasparenza e non discriminazione e che sia data evidenza della metodologia utilizzata e dell'iter procedurale seguito per l'effettuazione dell'acquisto, dell'oggetto, dell'importo e delle motivazioni sottese alla scelta del fornitore, il tutto secondo una specifica procedura;
- l'approvvigionamento di beni o servizi sia disciplinato da contratto o ordine scritto, nel quale sono chiaramente prestabiliti il prezzo del bene o della prestazione o i criteri per determinarlo;
- nella selezione di fornitori siano richieste, ove possibile, almeno 3 offerte;
- nella scelta del fornitore siano preventivamente valutati criteri soggettivi od oggettivi predefiniti, tra cui la reputazione e l'affidabilità del soggetto sul mercato, nonché l'adesione a valori comuni a quelli espressi dal Codice Etico e dal Modello di P&P Technology srl;
- la documentazione prodotta o ricevuta dell'acquisizione di beni o servizi sia conservata, ad opera dei Responsabili delle Funzioni coinvolte, in un apposito archivio, con modalità tali da impedire la modifica successiva al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi;
- il Responsabile della Funzione interessata dalla fornitura segnali immediatamente all'OdV eventuali anomalie nelle prestazioni rese dal fornitore o particolari richieste avanzate a P&P Technology srl da questi soggetti;
- tutti i pagamenti a fornitori siano effettuati solo dopo una validazione preventiva da parte del Responsabile della Funzione interessata dall'acquisto ed a seguito di un iter autorizzativo interno predefinito che tenga conto anche della scadenza del pagamento;
- l'utilizzo o l'impiego di risorse economiche o finanziarie abbia sempre una causale espressa e sia documentato e registrato in conformità ai principi di correttezza professionale e contabile;
- le fatture ricevute da P&P Technology srl relative all'acquisto di beni o servizi siano registrate esclusivamente a fronte di idonea evidenza della effettiva ricezione della merce o dell'avvenuta prestazione del servizio;

- per quanto possibile, non vi sia identità soggettiva tra chi richiede, chi autorizza, chi controlla e chi esegue le operazioni;
- gli impegni e i contratti stipulati con fornitori di beni selezionati siano firmati da soggetti dotati di idonei poteri;
- non siano corrisposti pagamenti a fornitori in misura non congrua rispetto alla natura ed al valore dei beni o servizi forniti, o non conformi alle condizioni commerciali o alle prassi esistenti sul mercato.

II. *Assegnazione di* ***consulenze e di prestazioni professionali****. I protocolli prevedono che:*

- i soggetti cui conferire incarichi di consulenza siano scelti in base ai requisiti di professionalità, indipendenza e competenza;
- l'individuazione di tali soggetti sia sempre motivata dalla Funzione richiedente o da ragioni organizzative;
- l'affidamento degli incarichi avvenga nel rispetto delle procedure, delle autorizzazioni e dei controlli interni adottati da P&P Technology srl, che devono prevedere i criteri per la definizione ed allocazione del budget e per la scelta della tipologia di prestazione più idonea;
- l'incarico sia conferito per iscritto con indicazione del compenso pattuito e del contenuto della prestazione;
- al termine dell'incarico sia richiesto al Consulente di dettagliare per iscritto le prestazioni effettuate, se non diversamente riscontrabili;
- al fine di autorizzare il pagamento della prestazione, la Funzione richiedente certifichi l'avvenuta prestazione prima del pagamento stesso;
- non siano corrisposti compensi in misura non congrua rispetto alle prestazioni rese a P&P Technology srl o non conformi all'incarico conferito, alle condizioni o prassi esistenti sul mercato o alle tariffe professionali vigenti per la categoria interessata.

III. *Gestione delle risorse finanziarie* ***(incassi e pagamenti)****;*

- l'Organo Amministrativo, o il soggetto da esso delegato, stabilisca e modifichi i limiti all'autonomo impiego delle risorse finanziarie;
- le operazioni che comportano l'utilizzo o l'impiego di risorse economiche o finanziarie abbiano una causale espressa, siano motivate dal soggetto richiedente, anche attraverso la mera indicazione della tipologia di spesa alla quale appartiene l'operazione, e siano documentate e registrate in conformità ai principi di correttezza professionale e contabile;
- siano vietati i flussi sia in entrata che in uscita in denaro contante, salvo che sia previsto dalla legge e per tipologie minime di spesa (piccola cassa) espressamente previste dalle Funzioni competenti;
- sia costantemente monitorato il credito verso terzi e verso le consorziate e le decisioni in merito ad eventuali transazioni, compensazioni ed in generale relative ai crediti in essere siano disposte solo dall'Organo Amministrativo o dal soggetto da questo delegato;
- in caso di flussi in entrata tramite assegni sia data evidenza:
- della corrispondenza del titolo di pagamento con uno specifico ordine di acquisto, quand'anche il titolo si riferisca ad una frazione relativa a pagamenti rateizzati;
- della corrispondenza del firmatario con l'effettivo acquirente o come legale rappresentante dello stesso.
- con riferimento alle operazioni bancarie e finanziarie, P&P Technology srl si avvalga solo di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea;

- i pagamenti a terzi siano effettuati mediante circuiti bancari con mezzi che garantiscano evidenza che il beneficiario del pagamento sia effettivamente il soggetto terzo contraente con P&P Technology srl;
- gli incassi e i pagamenti di P&P Technology srl nonché i flussi di denaro siano sempre tracciabili e provabili documentalmente.

IV. *Gestione delle **spese di rappresentanza**. I protocolli prevedono che:*

- il rimborso delle spese sostenute, che includono anche le spese di rappresentanza, debba essere richiesto attraverso la compilazione di modulistica specifica e solo previa produzione di idonea documentazione giustificativa delle spese sostenute;
- sia individuato, secondo i livelli gerarchici presenti in azienda, il responsabile che autorizza ex ante o ex post le note spese ai soggetti richiedenti;
- le spese di rappresentanza siano gestite secondo le modalità comunicate a tutto il personale, in termini di rispetto dei massimali di spesa, delle finalità delle spese sostenute, della modulistica, dei livelli autorizzativi richiesti e della liquidazione delle somme a rimborso.

***V*. *Selezione ed assunzione del personale** (e gestione dei beni come autovetture, cellulari, carte di credito, carta carburante). I protocolli prevedono che:*

- la definizione, in virtù delle esigenze relative al ruolo e alla mansione specifica che il soggetto sarà chiamato a svolgere, di criteri di idoneità del personale ricercato e di criteri oggettivi di selezione dei candidati;
- la verifica al momento dell'assunzione di requisiti professionali, reputazionali, di onorabilità/eventuali carichi pendenti (per quanto consentito dalla legge applicabile);
- in caso di assunzione di lavoratori di paesi terzi la verifica del rispetto della normativa in materia di immigrazione nel territorio dello Stato di destinazione, in particolare:
- l'identificazione di ruoli e responsabilità per la gestione delle attività (inclusi gli adempimenti verso i competenti soggetti pubblici) propedeutiche all'instaurazione del rapporto di lavoro subordinato;
- la verifica del possesso, da parte dei lavoratori provenienti da paesi terzi, di un permesso di soggiorno valido;
- il monitoraggio circa la scadenza, la revoca o l'annullamento di tale permesso
- siano identificati i beni e le utilità concessi (ad es. personal computer, telefono cellulare, ecc.);
- se necessario, venga mantenuto un inventario aggiornato dei beni attribuiti agli assegnatari;
- siano previsti casi di revoca del bene assegnato in caso di violazione delle procedure o regolamenti adottati da P&P Technology srl durante il loro utilizzo;

***VI*. *Operazioni di **sponsorizzazione ed erogazioni liberali**. I protocolli prevedono che:*

- le operazioni siano, oltre che mirate ad attività lecite ed etiche, anche autorizzate, giustificate e documentate;
- la documentazione di supporto alle operazioni effettuate sia conservata in un apposito archivio, con modalità tali da impedire la modifica successiva se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

***VII*. *Gestione dei **rapporti con i rappresentanti della PA** in occasione di accertamenti, ispezioni, verifiche. I protocolli prevedono che:*

- l'identificazione di un soggetto responsabile per la gestione dei rapporti con soggetti pubblici in caso di ispezioni, appositamente delegato dai vertici di P&P Technology srl;
- le modalità di trasmissione delle informazioni richieste da parte di soggetti pubblici
- l'identificazione dei ruoli, delle responsabilità e delle modalità di trasmissione delle informazioni relativamente a flussi di carattere continuativo e/o periodico, previsti dalla legge o imposti da soggetti pubblici;
- la formalizzazione relativa alle evidenze dell'incontro svolto e, almeno per i casi più significativi, delle riunioni e/o delle comunicazioni che intercorrono con i soggetti pubblici;
- l'obbligo di segnalazione iniziale e di relazione sulla chiusura delle attività di controllo e/o verifica con indicazione:
    - dei dati identificativi degli ispettori (nome ed ente di appartenenza);
    - della data e l'ora di arrivo degli ispettori;
    - della durata dell'ispezione;
    - dell'oggetto della stessa;
    - dell'esito della stessa;
    - dell'eventuale verbale redatto dell'ente ispettivo;
    - dell'elenco degli eventuali documenti consegnati.

Protocolli specifici di prevenzione e informative all'OdV

Oltre a quanto espressamente previsto dai precedenti protocolli con riferimento a specifiche Attività Sensibili, i Referenti di P&P Technology srl trasmettono all'OdV le ulteriori informazioni individuate nelle procedure o negli altri Strumenti di attuazione del Modello applicabili, con la periodicità e le modalità previste dagli stessi.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO PREDISPOSTO AI SENSI DEL D.LGS 231/2001

PARTE SPECIALE - 2

REATI SOCIETARI

STATO DI REVISIONE DEL DOCUMENTO

Approvato da: Andrea Perpignani, Amministratore Unico____	Data: 02/12/2025

Data revisione :

Descrizione del documento

Ai sensi dell'art. 6 comma 2, lett. a) del D.Lvo 231/01, P&P TECHNOLOGY SRL, attraverso un processo di mappatura dei rischi, di valutazione delle attività, dei controlli esistenti e del contesto aziendale in cui opera (cd. *control and risk self assessment)*, ha identificato i processi e le attività *sensibili* nell'ambito delle quali possano essere potenzialmente commessi i reati societari previsti dal D.Lvo 231/2001.

Per il contrasto al rischio di commissione di tali reati si richiama quanto disposto dal Modello Organizzativo Parte Generale approvato da P&P TECHNOLOGY SRL, e tutti i destinatari del Modello sono tenuti ad adottare regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento ed ai principi contenuti nel Codice Etico.

I principi individuati nel Codice Etico, che qui viene integralmente richiamato costituiscono presupposto e parte integrante dei presidi e delle Misure di controllo descritte nella presente Parte Speciale con riferimento alle diverse tipologie di destinatari e/o *stakeholders*, nell'ambito delle diverse aree di rischio individuate.

La presente Parte Speciale potrà essere aggiornata dal Presidente o dalla Direzione e tale aggiornamento sarà sottoposto a validazione da parte dell'OdV.

REATO PRESUPPOSTO: *art. 25-ter* D.Lgs. 231/01).

Reati societari

- *False comunicazioni sociali (art. 2621 c.c.);*
- *Fatti di lieve entità (art. 2621-bis c.c.);*
- *False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.);*
- *Impedito controllo che ha cagionato un danno ai soci (art. 2625, comma 2, c.c.);*
- *Operazioni in pregiudizio dei creditori (art. 2629 c.c.);*
- *Corruzione tra privati con riferimento anche all'induzione indebita a dare o promettere utilità (art. 2635 c.c.).*

Premessa

Sulla base delle analisi condotte sono considerati applicabili a P&P TECHNOLOGY SRL i seguenti reati societari:

art. 2621 c.c. false comunicazioni sociali. Sono costituite dalla condotta degli amministratori, dei direttori generali, dei dirigenti preposti alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore;

art. 2621-bis c.c. fatti di lieve entità. Sono costituite dalla condotta di chi commette i fatti previsti dall'art. 2621 c.c. in misura lieve, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta;

art. 2625 c.c. impedito controllo. E' costituito dalla condotta degli amministratori i quali, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali;

art. 2629 c.c operazioni in pregiudizio dei creditori. E' costituito dalla condotta degli amministratori i quali, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori;

art. 2635, comma 3, c.c. corruzione tra privati. E' costituito dalla condotta di colui che, anche per interposta persona, dà o promette denaro o altra utilità agli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o altri enti privati, nonché a coloro che sono sottoposti alla direzione o alla vigilanza di detti soggetti, affinché, per sé o per altri, compiano o omettano atti in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà;

Processi Aziendali

I reati previsti dagli artt. 25 ter e le attività sensibili indicate di seguito impattano sui seguenti processi:

- Pianificazione, Amministrazione, Controllo e gestione fiscale;
- Gestione dei fornitori
- Gestione del personale
- Relazioni Esterne
- Erogazione del servizio

Attività Sensibili

P&P Technology srl ha individuato le seguenti Attività Sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i citati reati societari previsti dall'art. 25-ter del Decreto:

I. Gestione del processo di acquisto di beni e servizi (inclusa selezione, qualifica e gestione fornitori);
II. Assegnazione di consulenze e di prestazioni professionali;
III. Gestione delle risorse finanziare (incassi e pagamenti);
IV. gestione del credito;
V. Rilevazione, registrazione e rappresentazione dell'attività nelle scritture contabili, nei bilanci nelle relazioni e in altri documenti, anche tramite consulenti esterni;
VI. Operazioni di sponsorizzazione ed erogazioni liberali;
VII. Gestione delle spese di rappresentanza;
VIII. Gestione dei rapporti con soggetti pubblici e privati e con le organizzazioni collegate;
IX. Selezione e assunzione del personale;
X. Gestione dei benefit (i.e. autovetture, cellulari, carte di credito, carta carburante).

Procedure e Misure di prevenzione

I. *Gestione del processo di acquisto di beni e servizi (inclusa selezione, qualifica e gestione fornitori). I protocolli prevedono che:*

- il Responsabile della Funzione coinvolta che approva l'accordo:
  - conservi la documentazione relativa all'operazione in un apposito archivio, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi;
  - informi l'OdV di qualsiasi criticità possa riscontrarsi.

II. – III.– VI – VII - VIII. -IX. –X. Assegnazione di consulenze e di prestazioni professionali, gestione delle risorse finanziare (incassi e pagamenti), operazioni di sponsorizzazione ed erogazioni liberali, gestione delle spese di rappresentanza, rapporti con soggetti pubblici e privati, selezione e assunzione del personale, gestione dei beni (i.e. autovetture, cellulari, carte di credito, carta carburante), si applica quanto previsto al paragrafo IV e V della presente Parte Speciale, con riferimento alle corrispondenti Attività Sensibili.

IV. – V. Gestione del credito, rilevazione, registrazione e rappresentazione dell'attività nelle scritture contabili, nei bilanci nelle relazioni e in altri documenti, anche tramite consulenti esterni. I protocolli prevedono che:

- P&P Technology srl opera in conformità ai principi contabili nazionali e sono indicati con chiarezza i dati e le notizie che ciascuna Funzione deve fornire nonché i criteri contabili per l'elaborazione dei dati e la tempistica per la loro trasmissione all'Organo amministrativo ed alle Funzioni responsabili;
- tutte le operazioni di rilevazione e registrazione delle attività, anche con riferimento all'eventuale circolante determinato dalla ricezione di assegni, eventualmente riferiti a pagamenti frazionati, siano effettuate con correttezza e nel rispetto dei principi di veridicità e completezza;
- i responsabili delle diverse Funzioni forniscano all'Organo Amministrativo le informazioni loro richieste in modo tempestivo e attestando, ove possibile, la completezza e la veridicità delle informazioni, o indicando i soggetti che possano fornire tale attestazione;
- qualora utile per la comprensione dell'informazione, i responsabili delle diverse Funzioni indichino i documenti o le fonti originarie dalle quali sono tratte ed elaborate le informazioni trasmesse, e, ove possibile, ne alleghino copia;
- la rilevazione, la trasmissione e l'aggregazione delle informazioni contabili finalizzate alla predisposizione delle comunicazioni avvengano esclusivamente tramite modalità che possano garantire la tracciabilità dei singoli passaggi del processo di formazione dei dati e l'identificazione dei soggetti;
- eventuali significative modifiche alle poste di bilancio o ai criteri di contabilizzazione delle stesse siano adeguatamente autorizzate secondo le procedure e le deleghe interne;
- la richiesta da parte di chiunque di ingiustificate variazioni dei criteri di rilevazione, registrazione e rappresentazione contabile o di variazione quantitativa dei dati rispetto a quelli già contabilizzati in base alle procedure operative di P&P Technology srl, sia oggetto di immediata comunicazione all'Organismo di Vigilanza;
- le bozze del bilancio e degli altri documenti contabili siano messi a disposizione dell'Organo Amministrativo con ragionevole anticipo rispetto alla data prevista per l'approvazione del bilancio

Protocolli specifici di prevenzione e informative all'OdV

Oltre a quanto espressamente previsto dai precedenti protocolli con riferimento a specifiche Attività Sensibili, i Referenti di ENTE trasmettono all'OdV le ulteriori informazioni individuate nelle procedure o negli altri Strumenti di attuazione del Modello applicabili, con la periodicità e le modalità previste dagli stessi.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO PREDISPOSTO AI SENSI DEL D.LGS 231/2001

PARTE SPECIALE - 3

OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

STATO DI REVISIONE DEL DOCUMENTO

Approvato da: Andrea Perpignani, Amministratore Unico____	Data: 02/12/2025

Data revisione :

Descrizione del documento

Ai sensi dell'art. 6 comma 2, lett. a) del D.Lvo 231/01, P&P Technology srl, attraverso un processo di mappatura dei rischi, di valutazione delle attività, dei controlli esistenti e del contesto aziendale in cui opera (cd. control and risk self assesment), ha identificato i processi e le attività sensibili (suddivise per tipologia di reato ed elencate nei paragrafi successivi), nell'ambito delle quali possano essere potenzialmente commessi reati di omicidio colposo / lesioni colpose gravi o gravissime con violazione delle norme antinfortunistiche previsti dal Decreto.

Per il contrasto al rischio di commissione di tali reati si richiama quanto disposto dal Modello Organizzativo Parte Generale approvato da P&P Technology srl, e tutti i destinatari del Modello sono tenuti ad adottare regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento ed ai principi contenuti nel Codice Etico, al fine di prevenire il verificarsi di reati previsti dal Decreto.

I principi individuati nel Codice Etico, che qui viene integralmente richiamato costituiscono presupposto e parte integrante dei presidi e delle Misure di controllo descritte nella presenta Parte Speciale con riferimento alle diverse tipologie di destinatari e/o stakeholders, nell'ambito delle diverse aree di rischio individuate.

La presente Parte Speciale potrà essere aggiornata dal Presidente o dalla Direzione e tale aggiornamento sarà sottoposto a validazione da parte dell'OdV.

REATO PRESUPPOSTO: art. 25-septies D.Lgs. 231/01).

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

- Omicidio colposo, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 589 c.p.);
- Lesioni personali colpose gravi o gravissime, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 590 c.p.).

Premessa

Le condotte penalmente rilevanti consistono nel fatto, da chiunque commesso, di cagionare la morte o lesioni gravi/gravissime al lavoratore, per effetto dell'inosservanza di norme antinfortunistiche. In linea teorica, soggetto attivo dei reati può essere chiunque sia tenuto ad osservare o far osservare le norme di prevenzione e protezione. Tale soggetto può quindi individuarsi, ai sensi del decreto 81/2008, nei datori di lavoro, nei dirigenti, nei preposti, nei soggetti destinatari di deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro, nonché nei medesimi lavoratori.

I delitti contemplati dagli artt. 589 e 590 c.p. sono caratterizzati dall'aggravante della negligente inosservanza delle norme antinfortunistiche. L'elemento soggettivo, dunque, consiste nella cd. colpa specifica, ossia nella volontaria inosservanza di norme precauzionali volte a impedire gli eventi dannosi previsti dalla norma incriminatrice.

Il concetto di colpa specifica rimanda all'art. 43 c.p., nella parte in cui si prevede che il delitto è colposo quando l'evento, anche se preveduto ma in ogni caso non voluto dall'agente, si verifica a causa dell'inosservanza di norme di leggi, regolamenti, ordini o discipline.

L’individuazione degli obblighi di protezione dei lavoratori deve considerare, oltre decreto 81/2008 e agli altri specifici atti normativi in materia, anche l’art. 2087 c.c., che impone al datore di lavoro di adottare tutte quelle misure che, secondo la particolarità del lavoro, l’esperienza e la tecnica, sono necessarie a tutelare l’integrità fisica dei lavoratori.

Tale norma non può però intendersi come prescrivente l'obbligo generale ed assoluto di rispettare ogni cautela possibile ed “innominata” ad evitare qualsivoglia danno, perché in tal modo significherebbe ritenere automatica la responsabilità del datore di lavoro ogni volta che il danno si sia verificato (Cass. civ., sez. lav., n. 3740/1995).

Prediligendo, inoltre, un approccio interpretativo sistematico che valuti il rapporto di interazione tra norma generale (art. 2087 c.c.) e singole specifiche norme di legislazione antinfortunistica previste dal decreto 81 del 2008, appare coerente concludere che:

- l’art. 2087 c.c. introduce l’obbligo generale contrattuale per il datore di lavoro di garantire la massima sicurezza tecnica, organizzativa e procedurale possibile;
- conseguentemente, l’elemento essenziale ed unificante delle varie e possibili forme di responsabilità del datore di lavoro, anche ai fini dell'applicabilità dell'art. 25-septies del decreto 231 del 2001, è uno solo ed è rappresentato dalla mancata adozione di tutte le misure di sicurezza e prevenzione tecnicamente possibili e concretamente attuabili (come specificato dall’art. 3, comma 1, lett. b), del decreto 81/2008), alla luce dell’esperienza e delle più avanzate conoscenze tecnico-scientifiche.

A specificare ulteriormente il generico dettato legislativo, può giovare la sentenza della Corte Costituzionale n. 312 del 18 luglio 1996 secondo cui l'obbligo generale di massima sicurezza possibile deve fare riferimento alle misure che nei diversi settori e nelle diverse lavorazioni, corrispondono ad applicazioni tecnologiche generalmente praticate e ad accorgimenti generalmente acquisiti, sicché penalmente censurata è solo la deviazione del datore di lavoro dagli standard di sicurezza propri, in concreto ed al momento, delle singole diverse attività produttive.

Il novero degli obblighi in materia antinfortunistica si accresce ulteriormente ove si consideri che secondo la migliore dottrina e la più recente giurisprudenza l’obbligo di sicurezza in capo al datore di lavoro non può intendersi in maniera esclusivamente statica quale obbligo di adottare le misure di prevenzione e sicurezza nei termini sopra esposti (forme di protezione oggettiva), ma deve al contrario intendersi anche in maniera dinamica implicando l’obbligo di informare e formare i lavoratori sui rischi propri dell’attività lavorativa e sulle misure idonee per evitare i rischi o ridurli al minimo (forme di protezione soggettiva).

Il datore di lavoro che abbia, secondo i criteri sopra esposti, adempiuto agli obblighi in materia di salute e sicurezza sul luogo di lavoro (sia generali ex art. 2087 c.c. che speciali ex decreto 81 del 2008), è responsabile del solo evento di danno che si sia verificato in occasione dell'attività di lavoro e abbia un nesso di derivazione effettiva con lo svolgimento dell’attività lavorativa.

La giurisprudenza prevede infatti una interruzione del nesso di causalità tra la condotta dell'agente e l’evento lesivo ogni qualvolta la condotta del lavoratore sia da considerare abnorme, ossia strana e imprevedibile e perciò stesso si ponga al di fuori di ogni possibilità di controllo da parte delle persone preposte all'applicazione delle misure di prevenzione contro gli infortuni sul lavoro.
Conseguentemente deve ritenersi che rimangano fuori dall’ambito di rilevanza normativa (ai fini della responsabilità civile e penale) gli infortuni derivanti dalla sussistenza del cd. rischio elettivo ossia il rischio diverso da quello a cui il lavoratore sarebbe ordinariamente esposto per esigenze lavorative ed abnorme ed esorbitante rispetto al procedimento di lavoro e che il lavoratore affronta per libera scelta con atto volontario puramente arbitrario per soddisfare esigenze meramente personali.

Il quadro sopra esposto, sia pure in termini di estrema sintesi, riferito alla complessità dei presupposti formali e sostanziali della responsabilità del datore di lavoro per violazione di norme antinfortunistiche, consente di concludere che di fatto, con l'entrata in vigore della legge 123 del 2007, ogni azienda dovrebbe considerare inaccettabile il "rischio" di incorrere, oltre che nelle responsabilità di matrice civile e penale tipiche della materia, anche nelle ulteriori sanzioni del decreto 231/01 per il fatto di non aver predisposto ed efficacemente attuato un idoneo Modello di Organizzazione, Gestione e Controllo.

Quest'ultimo, per essere efficacemente attuato, potrà utilmente essere integrato con il ''sistema" degli adempimenti aziendali nascenti dagli obblighi di prevenzione e protezione imposti dall'ordinamento legislativo (v. sopra) e, qualora presenti, con le procedure interne nascenti dalle esigenze di gestione della sicurezza sul lavoro.

Da qui l'opportunità che l'ente ponga in essere azioni mirate volte garantire la suddetta integrazione (anche in vista della successiva eventuale verifica da parte del Giudice) ed in particolare:

- effettuazione di una mappatura del rischio approfondita e orientata secondo le specificità dell'attività produttiva presa in considerazione;
- attenta verifica ed eventuale integrazione delle procedure interne di prevenzione ai sensi del decreto 231 in coerenza con la specificità dei rischi di violazione delle norme richiamate dall'art. 25-septies; a tal fine sarà importante tenere conto e armonizzare tutte le attività già svolte, anche in materia di gestione della sicurezza, evitando inutili quanto costose duplicazioni;
- valutazione ed individuazione dei raccordi tra i vari soggetti coinvolti nel sistema di controllo ai sensi del decreto 231 e delle normative speciali in materia di sicurezza e salute sui luoghi di lavoro, con particolare riferimento alla previsione di un sistema integrato di controllo riguardante il Responsabile dei servizi di prevenzione e protezione (RSPP o altro soggetto giuridicamente equivalente) qualificabile come controllo tecnico ¬operativo o di primo grado, e l'Organismo di Vigilanza.

Sotto il profilo soggettivo, l'omicidio o le lesioni rilevanti ai fini della responsabilità amministrativa degli enti dovranno essere realizzati mediante colpa: tale profilo di imputazione soggettiva può essere generico (violazione di regole di condotta cristallizzate nel tessuto sociale in base a norme di esperienza imperniate sui parametri della diligenza, prudenza e perizia) o specifico (violazione di regole di condotta positivizzate in leggi, regolamenti, ordini o discipline).

Gli articoli del Cod. Pen. sanzionano pertanto chiunque, per colpa, cagioni rispettivamente la morte di una persona ovvero le arrechi lesioni personali gravi o gravissime.

Per "lesione" si intende l'insieme degli effetti patologici costituenti malattia, ossia quelle alterazioni organiche e funzionali conseguenti al verificarsi di una condotta violenta: la lesione è grave se la malattia ha messo in pericolo la vita della vittima, ha determinato un periodo di convalescenza superiore ai quaranta giorni, ovvero ha comportato l'indebolimento permanente della potenzialità funzionale di un senso o di un organo. È gravissima se la condotta ha determinato una malattia probabilmente insanabile (con effetti permanenti non curabili) oppure ha cagionato la perdita totale di un senso, di un arto, della capacità di parlare correttamente o di procreare, la perdita dell'uso di un organo ovvero ha deformato o sfregiato il volto della vittima.

Ai fini dell'implementazione del Modello è necessario comunque considerare che:

- il rispetto degli standard minimi di sicurezza previsti dalla normativa specifica di settore non esaurisce l'obbligo di diligenza complessivamente richiesto;

- è necessario garantire l'adozione di standard di sicurezza tali da minimizzare (e, se possibile, eliminare) ogni rischio di infortunio e malattia, anche in base alle migliori tecnica e scienza conosciute, secondo le particolarità del lavoro;
- non esclude tutte le responsabilità in capo alla persona fisica o all'ente il comportamento del lavoratore infortunato che abbia dato occasione all'evento, quando quest'ultimo sia da ricondurre, comunque, alla mancanza o insufficienza delle cautele che, se adottate, avrebbero neutralizzato il rischio sotteso a un siffatto comportamento. La responsabilità è esclusa solo in presenza di comportamenti del lavoratore che presentino il carattere dell'eccezionalità, dell'abnormità o dell'esorbitanza rispetto al procedimento lavorativo, alle direttive organizzative ricevute e alla comune prudenza.

Sotto il profilo dei soggetti tutelati, le norme antinfortunistiche non tutelano solo i dipendenti, ma tutte le persone che legittimamente si introducono nei locali adibiti allo svolgimento della prestazione lavorativa.

Per quanto concerne i soggetti attivi, possono commettere queste tipologie di reato coloro che, in ragione della loro mansione, svolgono attività sensibili in materia; ad es.:

- il lavoratore che, attraverso le proprie azioni e/o omissioni, può pregiudicare la propria ed altrui salute e sicurezza;
- il dirigente ed il preposto, ai quali possono competere, tra gli altri, i compiti di coordinamento e supervisione delle attività, di formazione e di informazione;
- il datore di lavoro, quale principale attore nell'ambito della prevenzione e protezione;
- il progettista, al quale compete il rispetto dei principi di prevenzione in materia di salute e sicurezza sul lavoro, sin dal momento delle proprie scelte progettuali e tecniche;
- il fabbricante, l'installatore ed il manutentore che, nell'ambito delle rispettive competenze, devono assicurare il rispetto delle norme tecniche applicabili;
- il committente, al quale competono, secondo le modalità definite dalla normativa, la gestione ed il controllo dei lavori affidati in appalto.

Processi Aziendali

I reati previsti dall'art. 25 septies e le attività sensibili indicate di seguito impattano sui seguenti processi:

- Servizio di Prevenzione e Protezione
- Gestione forniture e acquisti

Attività Sensibili

P&P Technology srl ha reputato di attivare gli strumenti di controllo e di gestione previsti dalla norma D.Lvo 81/08:

- la valutazione dei rischi prevista in materia di tutela della salute e della sicurezza;
- l'organizzazione del Servizio di Prevenzione e Protezione

Attraverso la valutazione dei rischi si sono individuate le condizioni ove, ragionevolmente, è possibile si manifestino degli eventi lesivi. Il Servizio di Prevenzione e Protezione, affidato ad un Responsabile qualificato ed in possesso dei titoli previsti dalla Legge per il suo ruolo garantisce la manutenzione ed aggiornamento puntuale del sistema di prevenzione e la formazione permanente del personale.

Suddivisione delle attività

Le attività che possono potenzialmente originare i reati di cui all'art. 25-septies del Decreto, in quanto una loro omissione o un'inefficace attuazione potrebbe integrare una responsabilità colposa della Società, sono riportate di seguito. La loro individuazione è stata condotta in accordo con quanto previsto dall'art. 30, D.Lgs. 81/2008 e considerando i requisiti previsti dalla Norma UNI EN ISO 45.001/2018 cui il Modello è ispirato:

I. Individuazione delle disposizioni normative applicabili, a cui uniformarsi per il rispetto degli standard tecnico-strutturali;

II. Definizione delle risorse, dei ruoli e delle responsabilità per assicurare le attività finalizzate all'attuazione delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

III. Valutazione dei rischi e predisposizione delle conseguenti misure di prevenzione e protezione;

IV. Individuazione e gestione delle misure di protezione collettiva e/o individuale atte a contenere o ad eliminare i rischi;

V. Gestione delle emergenze, delle attività di lotta agli incendi e di primo soccorso;

VI. Gestione degli appalti;

VII. Attività di sorveglianza sanitaria;

VIII. Attività di informazione e formazione in tema di salute, sicurezza e igiene sul lavoro;

IX. Attività di comunicazione, partecipazione e consultazione, gestione delle riunioni periodiche di sicurezza, consultazione degli RLS

X. Controlli sugli acquisti, acquisizione di documentazioni e certificazioni obbligatorie di legge;

XI. Gestione della documentazione e dei sistemi di registrazione al fine di garantire la tracciabilità delle attività.

L'elenco delle Attività Sensibili è periodicamente aggiornato, in relazione a nuove ed eventuali esigenze di prevenzione, secondo le procedure previste dal Modello.

Principi generali di comportamento

Il Modello non intende sostituirsi alle prerogative e responsabilità di legge disciplinate in capo ai soggetti individuati dal D.Lgs. 81/2008 e dalla normativa ulteriormente applicabile nei casi di specie. Costituisce, invece, un presidio ulteriore di controllo e verifica dell'esistenza, efficacia ed adeguatezza della struttura e organizzazione posta in essere in ossequio alla normativa speciale vigente in materia di antinfortunistica e tutela della sicurezza e della salute nei luoghi di lavoro.

Tutti i destinatari del Modello, come individuati nella Parte Generale, adottano regole di condotta conformi ai principi contenuti nella Normativa Antinfortunistica al fine di prevenire il verificarsi dei reati di omicidio e lesioni colposi, sopra identificati.

In particolare, costituisce presupposto e parte integrante dei protocolli di prevenzione la documentazione relativa alla tutela ed alla sicurezza dei luoghi di lavoro (ivi compresi il Documento di Valutazione dei Rischi nonché le procedure di gestione delle emergenze) attraverso cui si individuano le situazioni ove ragionevolmente è possibile si manifestino degli eventi lesivi riconducibili all'attività lavorativa.

Protocolli specifici di prevenzione

Il Documento di Valutazione dei Rischi indica specifiche misure di prevenzione degli infortuni e delle malattie professionali; per quanto riguarda questi aspetti si rinvia interamente a tale elaborato.

Quanto alle misure di prevenzione per le attività a rischio di reato come sopra identificate, di quei comportamenti che potrebbero quindi integrare la responsabilità di P&P Technology srl in relazione a infortuni sul lavoro, il presente Modello è adottato ed attuato al fine di garantire l'adempimento di tutti i relativi obblighi giuridici.

Ai fini dell'adozione e dell'attuazione del presente Modello valgono i principi ed i protocolli sviluppati per il Sistema di Gestione sviluppato sulla Norma UNI EN ISO 45.001/2018 qui di seguito indicati.

I. Individuazione delle disposizioni normative applicabili, a cui uniformarsi per il rispetto degli standard tecnico-strutturali. I protocolli prevedono che:

- La conformità alle vigenti norme in materia (leggi, norme tecniche e regolamenti, ecc.) è assicurata attraverso:
- l'identificazione e l'accessibilità alle norme in materia applicabili all'organizzazione;
- l'aggiornamento legislativo;
- il controllo periodico della conformità alla normativa applicabile.

II. Definizione delle risorse, dei ruoli e delle responsabilità per assicurare le attività finalizzate all'attuazione delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori

- Per tutte le figure individuate per la gestione di problematiche inerenti salute e sicurezza nei luoghi di lavoro, sono predefiniti idonei requisiti tecnico-professionali che possono trarre origine anche da specifici disposti normativi; tali requisiti sono in possesso del soggetto preliminarmente all'attribuzione dell'incarico e possono essere conseguiti anche attraverso specifici interventi formativi; essi devono essere mantenuti nel tempo.
- L'attribuzione di specifiche responsabilità avviene, in data certa, attraverso la forma scritta definendo, in maniera esaustiva, caratteristiche e limiti dell'incarico e, se del caso, individuando il potere di spesa.

In generale, a titolo esemplificativo:

sono formalizzate le responsabilità di gestione, coordinamento e controllo all'interno di P&P Technology srl;

- sono correttamente nominati i soggetti previsti dalla normativa in materia di igiene e sicurezza dei luoghi di lavoro (ivi inclusi, nel caso di presenza di cantieri, i soggetti previsti dal titolo IV del D.Lgs. 81/2008) e sono loro conferiti correttamente i poteri necessari allo svolgimento del ruolo agli stessi assegnato;
- è costruito il sistema di deleghe, dei poteri di firma e di spesa in maniera coerente con le responsabilità assegnate;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale è congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti situazioni di rischio;
- non vi è identità soggettiva fra coloro che assumono o attuano le decisioni e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo;
- i soggetti preposti e/o nominati ai sensi della normativa vigente in materia di igiene e sicurezza dei luoghi di lavoro possiedono competenze adeguate ed effettive in materia.

III. Valutazione dei rischi e predisposizione delle conseguenti misure di prevenzione e protezione

- L'operazione di individuazione e di rilevazione dei rischi viene effettuata con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza. La normativa cogente ne attribuisce la competenza al datore di lavoro che si avvale del supporto di altri soggetti: il Responsabile del Servizio di Prevenzione e Protezione ed il medico competente previa consultazione del rappresentante dei lavoratori per la sicurezza.
- Tutti i dati e le informazioni che servono alla valutazione dei rischi e conseguentemente all'individuazione delle misure di tutela (ad es. documentazione tecnica, misure strumentali, esiti di sondaggi interni, ecc.) devono essere chiari, completi e rappresentare in modo veritiero lo stato di P&P Technology srl.
- I dati e le informazioni sono raccolti ed elaborati tempestivamente, sotto la supervisione del datore di lavoro, anche attraverso soggetti da questo individuati in possesso di idonei requisiti, certificabili nei casi previsti, di competenza tecnica e, se del caso, strumentale. A richiesta, insieme ai dati ed alle informazioni devono essere trasmessi anche gli eventuali documenti e le fonti da cui sono tratte le informazioni.
- La redazione del Documento di Valutazione dei Rischi e del piano delle misure di prevenzione e protezione è un compito non delegabile dal datore di lavoro e deve essere effettuata sulla base di criteri definiti preliminarmente, nel rispetto di quanto previsto dall'art. 28, D.Lgs. 81/2008. Detti criteri, costituenti integrazione di tale documentazione, contemplano, tra gli altri, i seguenti aspetti:
  - attività di routine e non routine;
  - attività di tutte le persone che hanno accesso al posto di lavoro (compresi esterni);
  - comportamento umano;
  - pericoli provenienti dall'esterno;
  - pericoli legati alle operazioni o creati nell'ambiente circostante;
  - infrastrutture, attrezzature e materiali presenti presso il luogo di lavoro;
  - modifiche apportate ai processi e/o al sistema di gestione, tra cui le modifiche temporanee, e il loro impatto sulle operazioni, processi ed attività;
  - eventuali obblighi giuridici applicabili in materia di valutazione dei rischi e di attuazione delle necessarie misure di controllo;

- progettazione di ambienti di lavoro, macchinari ed impianti;
- procedure operative e di lavoro.

IV. Individuazione e gestione delle misure di protezione collettiva e/o individuale atte a contenere o ad eliminare i rischi

- Conseguentemente alla valutazione dei rischi effettuata sia al momento della predisposizione del Documento di Valutazione dei Rischi sia in occasione della predisposizione dei piani operativi della sicurezza, al fine della mitigazione dei rischi, sono individuati i necessari presidi sia individuali sia collettivi atti a tutelare il lavoratore.
- Attraverso il processo di valutazione dei rischi si disciplina:
- l'identificazione delle attività per le quali prevedere l'impiego di DPI;
- la definizione dei criteri di scelta dei DPI, che devono assicurare l'adeguatezza dei DPI stessi alle tipologie di rischio individuate in fase di valutazione e la loro conformità alle norme tecniche vigenti (ad es. marcatura CE);
- la definizione delle modalità di consegna ed eventualmente di conservazione dei DPI;
- la definizione di un eventuale scadenzario per garantire il mantenimento dei requisiti di protezione.

V. Gestione delle emergenze, delle attività di lotta agli incendi e di primo soccorso

- La gestione delle emergenze è attuata attraverso specifici piani che prevedono:
- identificazione delle situazioni che possono causare una potenziale emergenza;
- definizione delle modalità per rispondere alle condizioni di emergenza e prevenire o mitigare le relative conseguenze negative in tema di salute e sicurezza;
- pianificazione della verifica dell'efficacia dei piani di gestione delle emergenze;
- aggiornamento delle procedure di emergenza in caso di incidenti o di esiti negativi delle simulazioni periodiche.
- Sono definiti specifici piani di gestione delle emergenze. Attraverso detti piani sono individuati i percorsi di esodo e le modalità di attuazione, da parte del personale, delle misure di segnalazione e di gestione delle emergenze.
- Tra il personale sono individuati gli addetti agli interventi di emergenza; essi sono in numero sufficiente e preventivamente formati secondo i requisiti di legge.
- Sono disponibili e mantenuti in efficienza idonei sistemi per la lotta agli incendi scelti per tipologia e numero in ragione della specifica valutazione del rischio di incendio ovvero delle indicazioni fornite dall'autorità competente; sono altresì presenti e mantenuti in efficienza idonei presidi sanitari.
- L'efficienza dei piani è garantita attraverso la periodica attività di prova, finalizzata ad assicurare la piena conoscenza da parte del personale delle corrette misure comportamentali e l'adozione di idonei strumenti di registrazione atti a dare evidenza degli esiti di dette prove e delle attività di verifica e di manutenzione dei presidi predisposti.

VI. Gestione degli appalti,

Le attività in appalto e le prestazioni d'opera sono disciplinate dall'art. 26 e dal Titolo IV del D.Lgs. 81/2008.

- Il soggetto esecutore delle lavorazioni deve possedere idonei requisiti tecnico-professionali, verificati anche attraverso l'iscrizione alla CCIAA. Esso dovrà dimostrare il rispetto degli obblighi assicurativi e previdenziali nei confronti del proprio personale, anche attraverso la presentazione del Documento Unico di Regolarità Contributiva. Se necessario, il soggetto esecutore deve inoltre presentare all'INAIL apposita denuncia per le eventuali variazioni totali o parziali dell'attività già assicurata (in ragione della tipologia di intervento richiesto e sulla base delle informazioni fornite da P&P Technology srl).
- L'impresa esecutrice, nei casi contemplati dalla legge, al termine degli interventi deve rilasciare la dichiarazione di conformità alle regole dell'arte.
- Con particolare riferimento a fornitori, installatori e manutentori esterni di macchinari, impianti e di qualsiasi tipo di presidio di sicurezza e attrezzature di lavoro da realizzarsi o installare all'interno di pertinenze poste sotto la responsabilità giuridica del datore di lavoro della Società, sono attuati specifici presidi di controllo che prevedono:
- procedure di verifica dei fornitori che tengono conto anche del rispetto da parte degli stessi e dei loro lavoratori delle procedure di sicurezza;
- definizione dell'ambito di intervento e degli impatti dello stesso all'interno di in un contratto scritto;
- definizione degli accessi e delle attività esercite sul sito da parte dei terzi, con valutazione specifica dei rischi interferenti legati alla loro presenza e relativa redazione della prevista documentazione di coordinamento (ad es. DUVRI, PSC) sottoscritta da tutti i soggetti esterni coinvolti e prontamente adeguata in caso di variazioni nei presupposti dell'intervento;
- clausole contrattuali in merito ad eventuali inadempimenti di lavoratori di terzi presso i siti aziendali relativamente alle tematiche sicurezza che prevedano l'attivazione di segnalazioni apposite;
- sistemi di rilevamento presenze di lavoratori terzi e di controllo sulle ore di lavoro effettivamente svolte e sul rispetto dei principi di sicurezza, come integrati eventualmente dai contratti;
- formalizzazione e tracciabilità del controllo da parte dei dirigenti e del datore di lavoro del rispetto dei presidi di controllo sin qui elencati.

VII. Attività di sorveglianza sanitaria

- Preliminarmente all'attribuzione di una qualsiasi mansione al lavoratore è necessario verificarne i requisiti sia per quanto riguarda gli aspetti tecnici (cfr. Attività Sensibile successiva: competenza, informazione, formazione e consapevolezza dei lavoratori), sia per quanto riguarda gli aspetti sanitari, se riscontrati in sede di valutazione del rischio.
- La verifica dell'idoneità è attuata dal medico competente che, in ragione delle indicazioni fornite dal datore di lavoro e sulla base della propria conoscenza dei luoghi di lavoro e delle lavorazioni, verifica preventivamente l'idoneità sanitaria del lavoratore rilasciando giudizi di idoneità totale o parziale ovvero di inidoneità alla mansione. In ragione della tipologia della lavorazione richiesta e sulla base degli esiti della visita preliminare, il medico competente definisce un protocollo di sorveglianza sanitaria a cui sottopone il lavoratore.

VIII. Attività di informazione e formazione in tema di salute, sicurezza e igiene sul lavoro

- Tutto il personale riceve opportune informazioni circa le corrette modalità di espletamento dei propri incarichi, è formato e, nei casi previsti dalla normativa, è addestrato. Di tale formazione e/o addestramento è prevista una verifica documentata. Le attività formative sono erogate attraverso modalità variabili (ad es. formazione frontale, comunicazioni scritte, ecc.) definite sia da scelte da P&P Technology srl sia da quanto previsto dalla normativa vigente.
- La scelta del soggetto formatore può essere vincolata da specifici disposti normativi.
- In tutti i casi le attività di informazione, formazione e addestramento sono documentate; la documentazione inerente la formazione del personale è registrata ed è impiegata anche al fine dell'attribuzione di nuovi incarichi.
- L'attività di formazione è condotta al fine di:
- garantire, anche attraverso un'opportuna pianificazione, che qualsiasi persona sotto il controllo dell'organizzazione sia competente sulla base di un'adeguata istruzione, formazione o esperienza;
- identificare le esigenze di formazione connesse con lo svolgimento delle attività e fornire una formazione o prendere in considerazione altre azioni per soddisfare queste esigenze;
- valutare l'efficacia delle attività di formazione o di altre azioni eventualmente attuate, e mantenere le relative registrazioni;
- garantire che il personale prenda coscienza circa l'impatto effettivo o potenziale del proprio lavoro, i corretti comportamenti da adottare, i propri ruoli e responsabilità.

IX. Attività di comunicazione, partecipazione e consultazione, gestione delle riunioni periodiche di sicurezza, consultazione dei rappresentanti dei lavoratori per la sicurezza

Le procedure che regolamentano il coinvolgimento e la consultazione del personale definiscono le modalità di:

- comunicazione interna tra i vari livelli e Funzioni dell'organizzazione;
- comunicazione con i fornitori ed altri visitatori presenti sul luogo di lavoro;
- ricevimento e risposta alle comunicazioni dalle parti esterne interessate;
- partecipazione dei lavoratori, anche a mezzo delle proprie rappresentanze, attraverso:
  - il loro coinvolgimento nell'identificazione dei pericoli, valutazione dei rischi e definizione delle misure di tutela;
  - il loro coinvolgimento nelle indagini relative ad un incidente;
  - la loro consultazione quando vi siano cambiamenti che possano avere significatività in materia di Salute e Sicurezza.

X. Controlli sugli acquisti, acquisizione di documentazioni e certificazioni obbligatorie di legge;

- Per le misure di prevenzione derivanti da questa attività, rinviamo, in quanto pertinenti, ai paragrafi successivi.

XI. Gestione della documentazione e dei sistemi di registrazione al fine di garantire la tracciabilità delle attività

- La gestione della documentazione costituisce un requisito essenziale ai fini del mantenimento del Modello; attraverso una corretta gestione della documentazione e l'adozione di sistemi di registrazione appropriati si coglie l'obiettivo di dare evidenza di quanto attuato anche assicurando la tracciabilità dei percorsi decisionali. È altresì rilevante garantire la disponibilità e l'aggiornamento della documentazione sia di origine interna sia di origine esterna (ad es. documentazione relativa a prodotti e sostanze). La gestione della documentazione sia di origine interna sia di origine esterna e la gestione

delle registrazioni, che costituiscono documentazione speciale, avviene assicurandone la disponibilità, la tracciabilità e la conservazione.

La gestione della documentazione comprende anche la registrazione delle verifiche effettuate sulle figure rilevanti per la salute e sicurezza sul lavoro, come descritto qui di seguito.

- Obblighi di vigilanza sui preposti (art. 19 D.Lgs. 81/2008)

Con particolare riferimento alla vigilanza sui preposti, P&P Technology srl attua specifici controlli che prevedono che il datore di lavoro, o persona dallo stesso delegata:

a) programmi ed effettui controlli a campione in merito all'effettiva istruzione ricevuta dai soggetti che accedono a zone che li espongono ad un rischio grave e specifico;

b) programmi ed effettui controlli a campione in merito alle segnalazioni di anomalie da parte dei preposti, nonché alle segnalazioni di anomalie relative a comportamenti dei preposti stessi;

c) effettui controlli in merito alle segnalazioni dei preposti relativamente ad anomalie su mezzi ed attrezzature di lavoro e sui mezzi di protezione individuale e su altre situazioni di pericolo, verificando le azioni intraprese dal dirigente per la sicurezza responsabile ed eventuali follow up successivi alle azioni intraprese;

d) effettui controlli in merito all'effettiva avvenuta fruizione da parte dei preposti della formazione interna appositamente predisposta.

- Obblighi di vigilanza sui lavoratori (art. 20 D.Lgs. 81/2008)

Con particolare riferimento alla vigilanza sui lavoratori interni, P&P Technology srl attua specifici controlli che prevedono che il datore di lavoro, o persona dallo stesso delegata:

a) programmi ed effettui controlli a campione in merito all'effettiva istruzione ricevuta dai lavoratori che accedono a zone che li espongono ad un rischio grave e specifico;

b) programmi ed effettui controlli a campione in merito alle segnalazioni di anomalie da parte dei preposti;

c) effettui controlli in merito all'effettiva avvenuta fruizione da parte dei lavoratori della formazione interna appositamente predisposta;

d) effettui controlli in merito all'effettiva sottoposizione dei lavoratori ai controlli sanitari previsti dalla legge o comunque predisposti dal medico competente.

- Obblighi di vigilanza sul medico competente (art. 25 D.Lgs. 81/2008)

Con particolare riferimento alla vigilanza sul medico competente, P&P Technology srl attua specifici controlli che prevedono che il datore di lavoro:

a) verifichi il possesso da parte del medico competente dei titoli e dei requisiti previsti dalla legge per lo svolgimento di tale funzione;

b) verifichi che il medico competente partecipi regolarmente alle riunioni di coordinamento con il RSPP, i rappresentanti dei lavoratori per la sicurezza e il datore di lavoro stesso, aventi ad oggetto le tematiche della sicurezza sui luoghi di lavoro, incluse quelle relative alle valutazioni dei rischi aziendali e quelle aventi un impatto sulla responsabilità sociale aziendale;

c) verifichi la corretta e costante attuazione da parte del medico competente dei controlli sanitari e delle procedure aziendali relative alla sorveglianza sanitaria.

- Ulteriori controlli specifici e comunicazioni con l'OdV

Sono istituiti ulteriori controlli specifici volti a fare in modo che il sistema organizzativo di P&P Technology srl, istituito ai sensi delle normative applicabili in materia di sicurezza dei luoghi di lavoro e di prevenzione degli infortuni, sia costantemente monitorato e posto nelle migliori condizioni possibili di funzionamento.

Per il controllo dell'effettiva implementazione delle disposizioni previste dal D.Lgs. 81/2008 e dalla normativa speciale vigente in materia di antinfortunistica, tutela della sicurezza e della salute nei luoghi di lavoro, è previsto che:

a) i soggetti qualificati come datore di lavoro, Responsabile del Servizio di Prevenzione e Protezione e medico competente aggiornino periodicamente l'OdV di P&P Technology srl in merito alle tematiche relative alla sicurezza sui luoghi di lavoro;

b) il Responsabile del Servizio di Prevenzione e Protezione ed il medico competente comunichino senza indugio le carenze, le anomalie e le inadempienze riscontrate;

c) il Responsabile del Servizio di Prevenzione e Protezione effettui incontri periodici con l'OdV di P&P Technology srl al fine di illustrare le più rilevanti modifiche che sono effettuate al Documento di Valutazione dei Rischi e alle procedure del sistema di gestione della sicurezza;

d) il personale, il rappresentante dei lavoratori per la sicurezza, il medico competente, il Responsabile del Servizio di Prevenzione e Protezione e il datore di lavoro possano segnalare all'OdV informazioni e notizie sulle eventuali carenze nella tutela della salute e sicurezza nei luoghi di lavoro;

e) il datore di lavoro si assicuri che siano nominati tutti i soggetti previsti dalla normativa di settore, che siano muniti di adeguate, chiare e sufficientemente specifiche deleghe, che dispongano delle competenze e qualità necessarie, che abbiano poteri, anche di spesa, sufficientemente adeguati all'incarico e che siano effettivamente esercitate le funzioni e le deleghe conferite;

f) l'OdV, nell'esercizio delle sue funzioni, possa richiedere l'assistenza dei responsabili della sicurezza nominati di P&P Technology srl, nonché di competenti consulenti esterni.

g) Procedure e Misure di prevenzione

- Il Datore di Lavoro mette a disposizione dei lavoratori, attrezzature conformi ai requisiti di sicurezza previsti dalle disposizioni legislative e regolamentari, idonee ai fini della salute e sicurezza e adeguate al lavoro da svolgere o adattate a tali scopi, che devono essere utilizzate conformemente alle disposizioni legislative di recepimento delle direttive comunitarie.
- Il Lavoratore per lavorare in Sicurezza 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, e deve conformare la sua azione lavorativa alla formazione, alle istruzioni e ai mezzi forniti dal Datore di Lavoro.

h) Attività di audit per la verifica periodica dell'applicazione e dell'efficacia delle procedure

- Ai fini delle attività di controllo sopra indicate sono condotte specifiche attività di audit, a cura dell'OdV, anche con la collaborazione dei soggetti aziendali competenti o di consulenti esterni.
- Tali attività di audit sono condotte anche in accordo con quanto previsto dalle procedure del Sistema di Gestione della Sicurezza che definiscono i principi dell'attività di audit, la gestione dei programmi di audit, la conduzione dell'audit come pure la competenza degli auditor.

L'attività di audit è svolta assicurando che:

a) gli audit interni siano condotti ad intervalli pianificati al fine di determinare se il sistema di gestione sia o meno correttamente attuato e mantenuto in tutte le sue parti e sia inoltre efficace per il conseguimento degli obiettivi dell'organizzazione;

b) eventuali scostamenti dal sistema siano prontamente gestiti;

c) siano trasmesse le informazioni sui risultati degli audit all'Organo dirigente e al datore di lavoro.

Protocolli specifici di prevenzione e informative all'OdV

Oltre a quanto espressamente previsto dai precedenti protocolli con riferimento a specifiche Attività Sensibili, i Referenti di P&P Technology srl trasmettono all'OdV le ulteriori informazioni individuate nelle procedure o negli altri Strumenti di attuazione del Modello applicabili, con la periodicità e le modalità previste dagli stessi.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO PREDISPOSTO AI SENSI DEL D.LGS 231/2001

PARTE SPECIALE - 4

RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA

STATO DI REVISIONE DEL DOCUMENTO

Approvato da: Andrea Perpignani, Amministratore Unico____	Data: 02/12/2025

Data revisione :

Descrizione del documento

Ai sensi dell'art. 6 comma 2, lett. a) del D.Lvo 231/01, P&P Technology srl, attraverso un processo di mappatura dei rischi, di valutazione delle attività, dei controlli esistenti e del contesto aziendale in cui opera (cd. control and risk self assessment), ha identificato i processi e le attività sensibili nell'ambito delle quali possano essere potenzialmente commessi i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita previsti dal D.Lvo 231/2001.

Per il contrasto al rischio di commissione di tali reati si richiama quanto disposto dal Modello Organizzativo Parte Generale approvato da P&P Technology srl, e tutti i destinatari del Modello sono tenuti ad adottare regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento ed ai principi contenuti nel Codice Etico.

I principi individuati nel Codice Etico, che qui viene integralmente richiamato costituiscono presupposto e parte integrante dei presidi e delle Misure di controllo descritte nella presente Parte Speciale con riferimento alle diverse tipologie di destinatari e/o stakeholders, nell'ambito delle diverse aree di rischio individuate.

La presente Parte Speciale potrà essere aggiornata dal Presidente o dalla Direzione e tale aggiornamento sarà sottoposto a validazione da parte dell'OdV.

REATO PRESUPPOSTO: art. 25-octies D.Lgs. 231/01).

a) Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648-ter 1 c. p.) L 15/12/2014 n. 186.

Premessa

Sulla base delle analisi condotte sono considerati applicabili a P&P Technology srl i seguenti reati:

Riciclaggio concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo. E' particolarmente insidiosa l'ipotesi di proventi di natura criminosa, che possono costituire una situazione di "reato di filiera" nel quale si può rimanere coinvolti anche in assoluta buona fede.

La tutela viene attuata con la tecnica della prevenzione per mezzo di apposite misure e obblighi di comportamento che, ad eccezione dei limiti all'uso del contante e dei titoli al portatore che sono applicabili alla generalità dei soggetti, riguardano una vasta platea di soggetti: banche, intermediari finanziari, professionisti, revisori contabili e operatori che svolgono attività il cui esercizio è subordinato a licenze, autorizzazioni, iscrizioni in albi/registri o dichiarazioni di inizio attività richieste da norme di legge (es. recupero crediti per conto terzi, custodia e trasporto di denaro contante, di titoli o valori con o senza l'impiego di guardie giurate, agenzie di affari in mediazione immobiliare, ecc.).

Nei confronti dei soggetti potenzialmente esposti, trovano applicazione gli obblighi in tema di adeguata verifica della clientela, tracciabilità delle operazioni, adeguata formazione del personale e segnalazione di operazioni sospette.

Tali obblighi coinvolgono i diversi organi di controllo di gestione - nell'ambito dell'ente destinatario della normativa -, tra cui l'Organismo di vigilanza, a vigilare sull'osservanza della normativa antiriciclaggio e a comunicare le violazioni delle relative disposizioni di cui vengano a conoscenza nell'esercizio dei propri compiti o di cui abbiano altrimenti notizia. Gli obblighi di comunicazione riguardano in particolar modo le possibili infrazioni relative alle operazioni di registrazione, segnalazione e ai limiti all'uso di strumenti di pagamento e di deposito (contante, titoli al portatore, conti e libretti di risparmio anonimi o con intestazioni fittizie) e sono destinati ad avere effetto sia verso l'interno dell'ente (titolare dell'attività o legale rappresentante) che verso l'esterno (autorità di vigilanza di settore, Ministero Economia e Finanze), fermo restando che il dovere di informativa dell'Organismo di vigilanza non può che essere parametrato alla funzione, prevista dall'art. 6, comma 1, lett. b) del decreto 231, di vigilare sul funzionamento e sull'osservanza dei modelli.

Autoriciclaggio si concretizza nell'attività di occultamento dei proventi derivanti da crimini commessi in proprio; si verifica soprattutto in conseguenza di particolari reati, tra cui, i più frequenti, l'evasione fiscale, la falsa fatturazione, la corruzione e l'appropriazione di beni sociali.

Processi Aziendali

I reati previsti dall'art. 25 octies e le attività sensibili indicate di seguito impattano sui seguenti processi:

- Amministrazione (in particolare, Tesoreria, Personale, Ufficio contratti/gare, ecc.)
- Commerciale
- Finanza
- Direzione acquisti;
- Marketing.

Attività Sensibili

- attività con soggetti terzi, relative ai rapporti instaurati tra P&P Technology srl e soggetti terzi:
- contratti di acquisto e/o di vendita con controparti;
- transazioni finanziarie con controparti;
- investimenti con controparti; sponsorizzazioni.
- rapporti con organizzazioni collegate:
- contratti di acquisto e/o di vendita;
- gestione dei flussi finanziari

Procedure di base e Misure di prevenzione

Verifica dell'attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari sulla base di alcuni indicatori di anomalia quali: dati pregiudizievoli pubblici - protesti, procedure concorsuali - o acquisizione di informazioni commerciali sulla azienda, sui soci e sugli amministratori tramite società specializzate; entità del prezzo sproporzionata rispetto ai valori medi di mercato; coinvolgimento di "persone politicamente esposte".

Verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni.

Determinazione dei requisiti minimi in possesso dei soggetti offerenti e fissazione dei criteri di valutazione delle offerte nei contratti standard.

Determinazione dei criteri di selezione, stipulazione ed esecuzione di accordi di joint-ventures con altre imprese per la realizzazione di investimenti, con trasparenza e tracciabilità delle operazioni connesse.

Adozione di adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.

Procedure e misure di prevenzione

Fornitori/Partner e Pagamenti

Ruoli coinvolti

- **Responsabile Acquisto (RAcq):** avvia la richiesta, raccoglie preventivi, verifica operatività/qualità, propone il fornitore.
- **Responsabile Amministrativa (RAm):** esegue controlli formali/amministrativi, verifica pagamenti e congruità documentale, archivia evidenze.
- **Amministratore Unico (AU):** approva il fornitore/partner nei casi previsti, autorizza i pagamenti e gestisce le escalation.

Output obbligatori (evidenze)

- Scheda Fornitore/Partner (anche in formato semplice: 1 pagina)
- Evidenze dei controlli (screenshot/visure/email/report)
- Tracciabilità decisionale (mail/verbale/annotazione di approvazione)

Verifica attendibilità commerciale e professionale di fornitori/partner

1. Avvio richiesta

- **RAcq** apre una richiesta di acquisto/partnership indicando:
  - oggetto (cosa si compra o accordo)
  - valore stimato e durata
  - motivazione (necessità operativa)
  - eventuali alternative identificate

2. Raccolta dati minimi del soggetto

- **RAcq** raccoglie e trasmette a **RAm**:
  - ragione sociale, sede, P.IVA/CF, contatti
  - nominativi amministratori/soci rilevanti (se disponibili)
  - coordinate bancarie (IBAN intestato al fornitore)
  - offerta/preventivo con condizioni economiche

3. Controlli "base" obbligatori (sempre)

- **RAm** esegue e archivia evidenza di:
  - verifica correttezza P.IVA/CF e coerenza anagrafica
  - presenza di sede/contatti verificabili (sito, email aziendale, recapiti)
  - coerenza tra intestazione offerta, contratto e soggetto pagato
- **RAcq** verifica e annota:
  - coerenza tecnica/qualitativa dell'offerta con la richiesta
  - capacità operativa (referenze, portfolio, casi d'uso, demo)

4. Controlli "anomalia" (attivati se scatta un campanello)

Se emerge **anche uno** dei seguenti indicatori:

- prezzo **sproporzionato** rispetto al mercato / forti sconti immotivati
- richiesta di pagamento a soggetto **diverso** dall'emittente (o conti esteri senza motivazione)
- urgenze anomale ("pagare subito", "conto diverso", "non mettere causale")
- struttura societaria opaca / cambi frequenti di denominazione o sede
- notizie negative pubbliche, protesti, procedure concorsuali (ove rilevabili)
- presenza/coinvolgimento di **persone politicamente esposte (PEP)** (se emerge da fonti pubbliche o dichiarazioni)
- fornitore proposto da intermediari non chiari

Allora:

- **RAm** effettua controlli rafforzati:
  - richiesta documenti integrativi (es. visura/attestazioni, referenze, dichiarazione titolare effettivo se rilevante)

    - verifica reputazionale tramite fonti pubbliche e/o provider specializzati *se proporzionato al valore*
    - verifica motivazione economica di eventuali scostamenti prezzo
- **RAm** informa **AU** allegando evidenze e propone:
    - "OK con condizioni"
    - "OK dopo integrazioni"
    - "STOP/Esclusione"

5. Decisione e approvazione

- **Soglie consigliate (modificabili nel MOG):**
    - fino a € X: approvazione **RAcq + RAm**
    - oltre € X / anomalie presenti / partnership: approvazione **AU**
- **AU**:
    - approva / richiede integrazioni / rigetta
    - se approva con condizioni: definisce vincoli (es. pagamento a SAL, anticipo limitato, clausole contrattuali)

6. Contratto/ordine e archiviazione

- **RAm** verifica che nel contratto/ordine ci siano almeno:
    - oggetto, importo, tempi, modalità di consegna
    - riferimenti del fornitore corretti
    - condizioni di pagamento tracciabili
- **RAm** archivia nel fascicolo (digitale) tutte le evidenze.

Verifica regolarità dei pagamenti (coincidenza ordinante/destinatario/controparte)

1. Ricezione documento di pagamento

- **RAm** riceve fattura/nota/debito e verifica:
  - intestazione corretta e coerente con contratto/ordine
  - descrizione prestazione coerente con quanto acquistato
  - importo e scadenze coerenti con accordi

2. Controllo "coincidenza soggetti"

- **RAm** controlla che:
  - il beneficiario del pagamento (intestatario IBAN) coincida con la controparte contrattuale
  - non vi siano richieste di pagare a soggetti terzi o conti personali
- Se **non coincide**:
  - **STOP automatico**
  - richiesta formale di chiarimenti + documentazione (motivazione, deleghe, cessione credito, ecc.)
  - escalation ad **AU** prima di qualsiasi pagamento

3. Controllo causale e tracciabilità

- **RAm** imposta causale chiara (es. "Fattura n. … del … – servizio …")
- Vietati:
  - pagamenti in contanti
  - causali generiche ("saldo", "varie")
  - frazionamenti artificiosi per evitare controlli

4. Autorizzazione pagamento

- **RAm** prepara proposta pagamento con:
  - fattura + ordine/contratto + evidenza ricezione prestazione (se applicabile)
  - esito controlli coincidenza e regolarità
- **AU** autorizza il pagamento (firma digitale/ok email tracciata).

5. Esecuzione e riconciliazione

- **RAm** esegue (o fa eseguire) pagamento e:
  - salva contabile/quietanza
  - riconcilia con estratto conto e fattura
  - archivia evidenze nel fascicolo fornitore

Requisiti minimi e criteri di valutazione offerte (contratti standard)

1. Definizione requisiti minimi (prima di chiedere preventivi)

- **RAcq + RAm** definiscono requisiti minimi (checklist):
  - requisiti tecnici/servizio
  - requisiti economici (range prezzo, modalità pagamento)
  - requisiti compliance (privacy, sicurezza, subfornitori)

2. Raccolta preventivi (ove possibile)

- **RAcq** raccoglie almeno:
  - 2 preventivi per spese sopra soglia interna (se praticabile)
  - oppure motivazione della scelta "fornitore unico"

3. Valutazione comparativa (scheda punteggio semplice)

- **RAcq** valuta qualità/tempi
- **RAm** valuta condizioni contrattuali/pagamenti/rischi
- **AU** interviene se oltre soglia o anomalie

4. Decisione motivata e tracciata

- scelta motivata (prezzo/qualità/affidabilità)
- archiviazione scheda e preventivi

Joint-venture/accordi con altre imprese (trasparenza e tracciabilità)

1. Avvio proposta

- **RAcq** raccoglie obiettivi, investimenti, ruoli e benefici attesi

2. Due diligence minima

- **RAm** effettua controlli base + eventuali controlli rafforzati (come punto 1)

3. Definizione accordo scritto

- **AU** assicura che l'accordo preveda:
  - ruoli e responsabilità
  - flussi finanziari tracciabili
  - regole su dati (privacy, proprietà, accessi)
  - clausola risolutiva in caso di condotte illecite

4. Monitoraggio periodico

- **RAm** verifica periodicamente:
  - coerenza pagamenti / fatturazioni / deliverable
  - eventuali anomalie o scostamenti

Anomalie fornitori

1. Pianificazione annuale (micro)

- **AU** pianifica 1 sessione annua (30–60 min) per **RAcq e RAm**

2. Contenuti minimi

- indicatori di anomalia (prezzo, soggetti terzi, urgenze, causali)
- corretto uso tracciabilità pagamenti
- gestione escalation e STOP

3. Evidenza formazione

- **RAm** conserva:
    - registro presenze (anche e-mail “partecipato”)
    - slide o memo formativo

Protocolli specifici di prevenzione e informative all’OdV

Oltre a quanto espressamente previsto dai precedenti protocolli con riferimento a specifiche Attività Sensibili, i Referenti di P&P Technology srl trasmettono all’OdV le ulteriori informazioni individuate nelle procedure o negli altri Strumenti di attuazione del Modello applicabili, con la periodicità e le modalità previste dagli stessi.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO PREDISPOSTO AI SENSI DEL D.LGS 231/2001

PARTE SPECIALE - 5

DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

STATO DI REVISIONE DEL DOCUMENTO

Approvato da: Andrea Perpignani, Amministratore Unico____	Data: 02/12/2025

Data revisione :

Descrizione del documento

Ai sensi dell'art. 6 comma 2, lett. a) del D.Lvo 231/01, P&P Technology srl, attraverso un processo di mappatura dei rischi, di valutazione delle attività, dei controlli esistenti e del contesto aziendale in cui opera (cd. *control and risk self assessment)*, ha identificato i processi e le attività *sensibili* nell'ambito delle quali possano essere potenzialmente commessi delitti in materia di violazione del diritto d'autore previsti dal D.Lvo 231/2001.

Per il contrasto al rischio di commissione di tali reati si richiama quanto disposto dal Modello Organizzativo Parte Generale approvato da P&P Technology srl, e tutti i destinatari del Modello sono tenuti ad adottare regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento ed ai principi contenuti nel Codice Etico.

I principi individuati nel Codice Etico, che qui viene integralmente richiamato costituiscono presupposto e parte integrante dei presidi e delle Misure di controllo descritte nella presente Parte Speciale con riferimento alle diverse tipologie di destinatari e/o *stakeholders*, nell'ambito delle diverse aree di rischio individuate.

La presente Parte Speciale potrà essere aggiornata dal Presidente o dalla Direzione e tale aggiornamento sarà sottoposto a validazione da parte dell'OdV.

REATO PRESUPPOSTO: *art. 25-novies* D.Lgs. 231/01).

Delitti in materia di violazione del diritto d'autore

- *Duplicare abusivamente per trarne profitto, importare, distribuire, vendere, detenere, concedere in locazione programmi per elaboratore (Art. 171 -bis);*
- *Duplicare, riprodurre, trasmettere o diffondere in pubblico abusivamente un'opera d'ingegno, letteraria, scientifica, didattica, musicale, multimediale (Art. 171 ter);*

Premessa

Sulla base delle analisi condotte sono considerati applicabili a P&P Technology srl i seguenti delitti in materia di violazione del diritto d'autore:

- **art. 171-*bis*, L. 22 aprile 1941, n. 633**, costituito dalla condotta di chi:
    - abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE);
    - utilizza qualsiasi mezzo inteso a consentire o facilitare la rimozione arbitraria o l'elusione di protezioni di un software;
    - al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati, esegue l'estrazione o il reimpiego della banca di dati, distribuisce, vende o concede in locazione una banca di dati;
- **art. 171-*ter*, L. 633/1941**, costituito dalla condotta di chi – tra l'altro – abusivamente duplica, riproduce, o diffonde in pubblico opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali e multimediali.

Processi Aziendali

I reati previsti dagli artt. 25 *ter* e le attività sensibili indicate di seguito impattano sui seguenti processi

- *Gestione acquisti*
- *Relazioni Esterne*

Attività Sensibili

P&P Technology srl ha individuato le seguenti Attività Sensibili, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i citati delitti in materia di violazione del diritto d'autore previsti dall'art. 25-*novies* del Decreto:

- *Gestione della comunicazione, social media, pubblicità, promozione e marketing;*
- *Gestione del processo di acquisto di beni e servizi (inclusa selezione, qualifica e gestione fornitori);*
- *Formazione;*
- *Erogazione dei servizi.*

Protocolli di base e Misure di prevenzione

Per le operazioni riguardanti la **gestione della comunicazione, social media, pubblicità, promozione e marketing** e la **gestione del processo di acquisto di beni e servizi (inclusa selezione, qualifica e gestione fornitori)**, i protocolli prevedono che:

- le opere protette da diritto d'autore acquistate da P&P Technology srl ai fini dell'attività comunicativa siano catalogate in apposite cartelle;
    - sia previsto uno strumento normativo e/o organizzativo che regolamenti l'utilizzo, la conservazione e la distribuzione di testi (letterari, scientifici o didattici), musiche, disegni, immagini (statiche o in movimento), fotografie, programmi per elaboratore, banche di dati, protetti dal diritto d'autore (le "Opere"). In particolare, tale strumento deve:

a) prevedere meccanismi autorizzativi per l'utilizzo, la riproduzione, l'elaborazione, la duplicazione e la distribuzione di Opere o di parti delle stesse;

b) regolamentare l'adozione di strumenti di protezione (es. diritti di accesso) relativi alla conservazione e all'archiviazione di Opere assicurandone l'inventariazione;

c) sancire il divieto di porre in essere condotte che possano comportare la violazione delle prescrizioni dettate dalla normativa in materia di tutela del diritto morale e patrimoniale d'autore, e, tra l'altro, vietare le seguenti condotte:

a. in generale, il procurarsi illegalmente, nonché l'illecita conservazione, utilizzo, riproduzione, duplicazione, elaborazione, diffusione e distribuzione di Opere ottenute in violazione delle norme in materia di tutela del diritto d'autore;

b. l'illecita diffusione al pubblico anche attraverso reti telematiche di Opere o di parti di esse;

c. l'usurpazione della paternità di Opere, nonché la loro deformazione, mutilazione o altra modificazione da cui consegua una lesione dell'onore e della reputazione dell'autore;

d. la duplicazione illegale di programmi per elaboratore;

e. l'illecita riproduzione, trasferimento, distribuzione e/o comunicazione del contenuto di banche dati.

- per le opere delle quali sono state acquisite le licenze d'uso, il *database* comprende anche i seguenti dati:
    - data di acquisto della licenza;
    - data di scadenza della licenza;
    - tipo di utilizzo autorizzato dal contratto di licenza (ad es. *upload* su sito internet, diffusione in pubblico, utilizzo per *brochure* e relativo numero di copie massime utilizzabili, ecc.);
    - siano definiti e attivati criteri e modalità per controllare l'accesso da parte degli utenti a siti di download di contenuti;
    - siano definiti i criteri e le modalità per la gestione dei sistemi *software* che prevedano la compilazione e manutenzione di un inventario aggiornato del *software* in uso;
    - siano definiti e attivati criteri e modalità per controllare l'acquisto e l'uso di software formalmente autorizzato e certificato e sia prevista l'effettuazione di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di

controllare la presenza di software proibiti e/o non licenziati e/o potenzialmente nocivi;

- la documentazione a supporto dei controlli effettuati sia conservata, in un apposito archivio, con modalità tali da impedire la modifica successiva se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi;
- le applicazioni tengano traccia delle modifiche ai dati ed ai sistemi compiute dagli utenti;
- qualora la gestione della presente attività sia affidata *in outsourcing*, i contratti che regolano i rapporti con i fornitori del servizio prevedano apposite clausole che impongano:
- per i fornitori di *software*, la conformità dei software forniti a leggi e normative ed in particolare alle disposizioni di cui alla L. 633/1941;
- per le agenzie di *marketing* che supportano P&P Technology srl, il rispetto da parte delle stesse di leggi e normative di riferimento ed in particolare delle disposizioni di cui alla L. 633/1941;
- la manleva per P&P Technology srl in caso di violazioni commesse dai fornitori del servizio

Procedure e misure di prevenzione

Gestione comunicazione/marketing e acquisto/uso di Opere, contenuti digitali e software (tutela diritto d'autore – L. 633/1941)

La presente procedura disciplina, in modo **snello e operativo**, la gestione di: comunicazione, social media, pubblicità, promozione e marketing, nonché il processo di **acquisto, selezione e gestione fornitori** collegato (agenzie, grafici esterni, fotografi, piattaforme, banche immagini, software). Obiettivo: prevenire condotte che possano integrare violazioni del diritto d'autore e/o uso di software non autorizzato, assicurando **autorizzazioni, inventariazione, tracciabilità e conservazione delle evidenze**.

Ruoli coinvolti

- **Responsabile Grafico (RG)** – *ruolo principalmente coinvolto*: crea e pubblica contenuti, richiede asset e software, cura catalogazione e registro opere/software.
- **Responsabile Amministrativo (RA)**: gestisce acquisti e pagamenti, conserva contratti/licenze/fatture, supporta controlli periodici.
- **Amministratore Unico (AU)**: approva acquisti/licenze fuori soglia o ad alto rischio (agenzie/fornitori nuovi, licenze complesse), gestisce escalation e autorizzazioni straordinarie.

Regole generali e divieti

È vietato a tutti i destinatari (in particolare RG) di porre in essere condotte che comportino:

- procurarsi o usare **Opere** (testi, immagini, video, musica, foto, font, template, clip, grafiche, software, banche dati) **senza licenza** o in violazione dei termini;
- **diffondere al pubblico** (anche via web/social) Opere o parti di esse senza autorizzazione;
- **usurpare paternità** dell'Opera o modificarla in modo lesivo dell'onore/reputazione dell'autore;
- duplicare/installare **software non licenziato** o scaricato da fonti non autorizzate;
- riprodurre/trasferire/distribuire il contenuto di **banche dati** senza titolo.

Principio base: "Se non ho licenza/contratto/evidenza di utilizzo, non pubblico e non uso."

Procedure operative (Contenuti, Opere e licenze)

2.1 Acquisizione di Opere (immagini, video, musiche, testi, font, template, stock, ecc.)

1. **RG identifica il bisogno** (es. immagine per campagna, musica per video, font per brochure).
2. **RG verifica se esiste già un'Opera autorizzata** nel Catalogo Opere (vedi Scheda 1).
    - Se sì: usa solo nei limiti d'uso indicati.
3. Se l'Opera non esiste: **RG richiede acquisto/licenza** a **RA** inviando:
    - link o riferimento dell'Opera

- canale di utilizzo previsto (social, sito, brochure, LMS, ads…)
- quantità stimata (es. copie brochure, durata campagna)

4. **RA effettua l'acquisto** (o valida l'acquisto effettuato su piattaforme autorizzate) e conserva:
   - fattura/ricevuta
   - contratto/licenza o condizioni d'uso (PDF/screenshot)
5. **RG cataloga l'Opera** entro 2 giorni lavorativi in cartella dedicata e aggiorna il **Catalogo Opere** con i dati minimi:
   - data acquisto
   - scadenza licenza (se presente)
   - utilizzi consentiti (es. upload sito, social, ADS, copie max, uso commerciale, territori, durata)
   - fonte/fornitore e riferimento documento licenza
6. **Controllo pre-pubblicazione (RG)**: prima della pubblicazione/diffusione, RG verifica che:
   - l'uso previsto sia compreso nei termini di licenza
   - siano rispettati eventuali obblighi (attribuzione autore, watermark, divieti di modifica, limitazioni territoriali)
7. **Pubblicazione**: RG pubblica solo tramite account/sistemi aziendali autorizzati (no account personali).

2.2 Eventuale utilizzo di Opere fornite da terzi (agenzie/fornitori esterni)

1. **RG richiede al fornitore** una dichiarazione/e-mail con: "i materiali consegnati sono originali o regolarmente licenziati per l'uso concordato".
2. **RA archivia** la dichiarazione + contratto/ordine.
3. **RG cataloga** anche questi materiali nel Catalogo Opere indicando: "Fonte: fornitore X – licenza dichiarata/contrattuale".

2.3 Modifiche, elaborazioni, adattamenti

1. Se l'Opera viene modificata (ritaglio, montaggio, remix, adattamento font/template): **RG verifica** che la licenza consenta elaborazioni e opere derivate.
2. Se non è chiaro: **RG blocca l'uso** e chiede valutazione a **RA**; se rischio alto o licenza complessa → escalation **AU**.

Controllo accessi a siti di download e canali autorizzati

Regole minime

- Sono consentiti download di contenuti solo da:
  - piattaforme con **licenza tracciabile** (es. stock images/music con account aziendale)

    - fornitori contrattualizzati
- È vietato usare siti “free” non verificati o download via canali non ufficiali.

Operatività a carico di RG e RA

1. **RG mantiene una “Lista Fonti Autorizzate”** (max 10 voci) con: nome piattaforma, link, tipo contenuti, account aziendale usato.
2. **RA verifica annualmente** che:
    - gli abbonamenti/licenze siano attivi
    - gli account siano intestati all’azienda
3. Se RG ha bisogno di una nuova fonte: **richiesta a RA** → valutazione → approvazione **AU** se piattaforma nuova o licenza complessa.

Procedura software: inventario, acquisto autorizzato e verifiche

4.1 Acquisto e installazione software (solo autorizzato)

1. **RG richiede software/plug-in/font software** a **RA**, indicando:
    - nome software, versione
    - finalità d'uso
    - modello licenza (mensile/annuale/perpetua) e n. utenti/dispositivi
2. **RA acquista** solo da canali ufficiali e conserva:
    - fattura
    - licenza/contratto
    - credenziali/licenza key (se presenti) in archivio sicuro
3. **AU approva** quando:
    - nuovo software non standard
    - spesa sopra soglia interna (consigliata)
    - licenza con condizioni complesse (redistribuzione, multi-sede, uso commerciale esteso)
4. **RG installa** solo software acquistato/approvato e aggiorna **Inventario Software** (Scheda 2).

4.2 Verifica annuale software installati

- **Frequenza:** annuale.

1. **RG e AU esportano elenco software** dal PC (screenshot elenco app o elenco dal sistema).
2. **RA confronta** elenco con Inventario Software fatture messe da fornitori:
    - se match → OK
    - se software non presente o dubbio → **azione correttiva**
3. **Azione correttiva**:
    - RG disinstalla software non autorizzato entro 48 ore
    - RA aggiorna evidenza (screenshot disinstallazione)
    - se sospetto di software nocivo → informare AU e attivare supporto tecnico esterno

Tracciabilità, conservazione evidenze e "archivio non modificabile"

Struttura cartelle (cloud aziendale)

Creare una cartella "**Compliance – Opere e Licenze**" con sottocartelle:

- 01_Catalogo_Opere (file registro)
- 02_Licenze_e_Contratti (PDF, screenshot)
- 03_Evidenze_Pubblicazioni (opzionale: link o screenshot post/campagne)
- 04_Inventario_Software
- 05_Verifiche_Periodiche (check trimestrali)
- 06_Fornitori_Marketing (contratti, dichiarazioni)

Regola pratica anti-modifica:

- RA imposta permessi: RG può caricare/aggiornare i registri, ma i documenti "Licenze e Contratti" sono **sola lettura** dopo il caricamento (modifica solo RA).
- Ogni aggiornamento registro deve lasciare traccia (versioning cloud o log modifiche).

Outsourcing: clausole minime nei contratti (agenzie marketing / software / creativi)

Quando l'attività è affidata a terzi, **RA** inserisce (anche in forma di clausola breve nell'ordine/contratto) che il fornitore:

- garantisce conformità alle normative e in particolare alla **L. 633/1941**;
- garantisce che i materiali consegnati sono originali o regolarmente licenziati per gli usi concordati;
- si impegna a fornire, su richiesta, evidenze delle licenze o liberatorie;
- manleva P&P Technology srl per usi non autorizzati imputabili al fornitore (compatibilmente con il contratto).

AU approva contratti con agenzie/fornitori nuovi o strategici.

Controlli periodici e gestione non conformità

Controllo trimestrale (RA + RG +AU – 30/45 minuti)

- RA e AU verifica:
    - 5 opere a campione: evidenza licenza presente? uso conforme?
    - inventario software vs software installati
    - nuove fonti di download: autorizzate?
- Output: "Verbale/Check-list trimestrale" (Scheda 3).

Gestione non conformità (quando emerge un problema)

1. **STOP immediato** dell'uso/pubblicazione del contenuto o del software dubbio.
2. **RG** rimuove contenuti non conformi (se già pubblicati) appena possibile.

3. **RA** valuta azioni correttive:
    - acquisire licenza corretta oppure sostituire l'Opera
    - disinstallare software / regolarizzare licenza
4. Se l'evento è grave o ripetuto → **AU** valuta ulteriori misure (richiamo formativo, aggiornamento procedura, eventuale azione disciplinare).

Schede di controllo

Scheda 1 – Catalogo Opere e Licenze (registro)

Campi minimi:

- ID Opera
- Titolo/descrizione
- Fonte (piattaforma/fornitore)
- Data acquisto
- Scadenza licenza (se presente)
- Utilizzi consentiti (sito/social/ads/brochure copie max/territorio/durata)
- Obblighi (attribuzione, divieti modifica, watermark)
- File licenza/contratto (link interno)
- Responsabile inserimento (RG/RA)
- Note

Scheda 2 – Inventario Software

Campi minimi:

- Nome software
- Versione
- Dispositivo/utente (RG o postazione)
- Tipo licenza (abbonamento/perpetua)
- Data acquisto
- Scadenza
- Canale acquisto (vendor ufficiale)
- Evidenza licenza/fattura (link)
- Note (plugin inclusi, n. seats)

Scheda 3 – Check-list Verifica Trimestrale (RA + RG)

Sezioni:

- Opere: campione n. __ verificato (licenza presente / uso conforme / scadenze)
- Software: elenco installato verificato (OK / anomalie / azioni)
- Fonti download: solo autorizzate (OK / nuove fonti)
- Archiviazione evidenze: completa e in sola lettura (OK / integrazioni)
- Azioni correttive e responsabile / data chiusura

Protocolli specifici di prevenzione e informative all'OdV

Oltre a quanto espressamente previsto dai precedenti protocolli con riferimento a specifiche Attività Sensibili, i Referenti di P&P Technology srl trasmettono all'OdV le ulteriori informazioni individuate nelle procedure o negli altri Strumenti di attuazione del Modello applicabili, con la periodicità e le modalità previste dagli stessi.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO PREDISPOSTO AI SENSI DEL D.LGS 231/2001

PARTE SPECIALE - 6

REATI AMBIENTALI

STATO DI REVISIONE DEL DOCUMENTO

Approvato da: Andrea Perpignani, Amministratore Unico____	Data: 02/12/2025

Data revisione :

Descrizione del documento

Ai sensi dell'art. 6 comma 2, lett. a) del D.Lvo 231/01, P&P Technology srl, attraverso un processo di mappatura dei rischi, di valutazione delle attività, dei controlli esistenti e del contesto aziendale in cui opera (cd. *control and risk self assessment)*, ha identificato i processi e le attività *sensibili* (suddivise per tipologia di reato ed elencate nei paragrafi successivi), nell'ambito delle quali possano essere potenzialmente commessi reati ambientali previsti dal Decreto.

Per il contrasto al rischio di commissione di tali reati si richiama quanto disposto dal Modello Organizzativo Parte Generale approvato da P&P Technology srl, e tutti i destinatari del Modello sono tenuti ad adottare regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento ed ai principi contenuti nel Codice Etico, al fine di prevenire il verificarsi di reati previsti dal Decreto.

I principi individuati nel Codice Etico, che qui viene integralmente richiamato costituiscono presupposto e parte integrante dei presidi e delle Misure di controllo descritte nella presenta Parte Speciale con riferimento alle diverse tipologie di destinatari e/o *stakeholders*, nell'ambito delle diverse aree di rischio individuate.

La presente Parte Speciale potrà essere aggiornata dal Presidente o dalla Direzione e tale aggiornamento sarà sottoposto a validazione da parte dell'OdV.

REATO PRESUPPOSTO: *art. 25-undecies* D.Lgs. 231/01.

Reati ambientali

- *Inquinamento ambientale (art. 452-bis c.p.);*
- *Disastro ambientale (art. 452-quater c.p.)*
- *Delitti colposi contro l'ambiente (art. 452-quinquies c.p.)*
- *Circostanze aggravanti (art. 452-octies c.p.)*

Premessa

L'Unione Europea ha mostrato preoccupazione per la diffusione degli illeciti in materia ambientale, i cui effetti spesso si propagano anche oltre le frontiere degli Stati in cui i reati vengono commessi. Ha dunque imposto agli Stati membri di perseguire penalmente condotte che "provochino o possano provocare" pregiudizi all'ambiente e siano tenute "intenzionalmente o per grave negligenza". Per le sole "gravi violazioni" della disciplina europea in materia ambientale, i legislatori nazionali sono stati vincolati a introdurre sanzioni efficaci, proporzionate e dissuasive sia per la persona fisica che per P&P Technology srl.

Punti cardine della disciplina europea sulla tutela penale dell'ambiente sono dunque tre:

- l'incriminazione di gravi violazioni, dannose o almeno concretamente pericolose per l'ambiente;
- la commissione dei reati con dolo o grave negligenza;
- la previsione di sanzioni caratterizzate da efficacia, proporzionalità e dissuasione.

Anzitutto, dei reati ambientali presupposto di responsabilità ai sensi del decreto 231 solo alcuni sono concepiti come reati di danno o di pericolo concreto; altri incriminano condotte espressive di un pericolo meramente astratto, nel quadro di una impostazione giuridica e culturale che considera il bene ambiente caratterizzato da un substrato empirico che consente di apprezzare l'effettiva sussistenza di una lesione in termini di pericolo o di danno.

Diversi reati ambientali, poi, colpiscono violazioni meramente formali, e comunque la maggior parte dei reati richiamati è sanzionabile anche a titolo di colpa. In base a questa disciplina, dunque, gli illeciti ambientali in prevalenza sono punibili indipendentemente dal grado di colpa con cui sono commessi, anche se l'agente ha agito per semplice imprudenza o imperizia.

Una simile estensione dell'area del penalmente rilevante si riflette in punto di responsabilità da reato degli enti. I modelli organizzativi, infatti, per aspirare al riconoscimento di efficacia esimente, qualora si verifichino reati ambientali, devono contemplare misure idonee a evitare la commissione di un illecito **anche solo per negligenza o imprudenza**.

Processi Aziendali

I reati previsti dagli artt. 25 *undecies* e le attività sensibili indicate di seguito impattano sui seguenti processi:

- *Amministrazione, Controllo, Pianificazione;*
- *Relazioni Esterne*
- *Erogazione dei servizi*

Attività Sensibili

La società P&P TECHNOLOGY SRL ha individuato le seguenti Attività Sensibili e strumentali, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i citati reati nei rapporti con la P.A. previsti dagli artt. 24 e 25 del Decreto:

I. Rifiuti elettronici
II. Rifiuti urbani;
III. Emissioni;

Protocolli e Misure di Prevenzione

Gestione del processo di acquisto di beni e servizi

Con riferimento al processo di acquisto di beni e servizi, inclusa la selezione, qualifica e gestione dei fornitori e delle prestazioni professionali, P&P Technology srl applica quanto pertinente delle previsioni di cui al paragrafo a.4. della presente Parte Speciale.

In particolare, nella selezione dei fornitori incaricati della gestione dei rifiuti elettronici (RAEE) e dei servizi connessi, P&P Technology srl verifica preventivamente che gli stessi siano in possesso delle **autorizzazioni previste dalla normativa vigente**, assicurando la tracciabilità delle operazioni e la conservazione della relativa documentazione.

Rapporti con i rappresentanti della Pubblica Amministrazione

I rapporti con i rappresentanti della Pubblica Amministrazione sono improntati ai principi di **collaborazione, correttezza e trasparenza**.
La gestione dei rapporti è demandata all'Amministratore Unico, con il supporto del Responsabile Amministrativo per la messa a disposizione della documentazione richiesta.

Misure di prevenzione specifiche – Gestione dei rifiuti

3.1 Ambito e tipologie di rifiuti

Considerata la natura della società P&P Technology, le attività aziendali generano esclusivamente le seguenti tipologie di rifiuti:

- **rifiuti elettronici (RAEE)** derivanti dalla dismissione di apparecchiature informatiche e d'ufficio;
- **rifiuti urbani** assimilabili agli urbani;
- **emissioni** riconducibili alle normali attività d'ufficio, di entità trascurabile e non soggette ad autorizzazioni specifiche.

P&P Technology srl **non svolge attività produttiva** e **non genera rifiuti speciali industriali**.

Caratterizzazione e classificazione dei rifiuti

Procedura operativa

La caratterizzazione e classificazione dei rifiuti avviene secondo le seguenti modalità:

- **identificazione del rifiuto**, a cura del Responsabile Amministrativo, sulla base della tipologia e dell'origine del bene dismesso;
- **classificazione del rifiuto** come rifiuto elettronico (RAEE) o rifiuto urbano, in funzione delle caratteristiche del materiale;
- **registrazione del rifiuto** in apposita documentazione interna, con indicazione della tipologia, della data di generazione e della modalità di gestione prevista;
- **verifica della coerenza** tra la classificazione del rifiuto e la documentazione fornita dal soggetto incaricato del ritiro e dello smaltimento, ove prevista dalla normativa applicabile.

Per i rifiuti elettronici, la corretta classificazione è effettuata sulla base delle indicazioni normative e delle informazioni fornite dai fornitori autorizzati incaricati del recupero o smaltimento.

Deposito temporaneo dei rifiuti

Il deposito temporaneo dei rifiuti è gestito nel rispetto dei seguenti criteri:

- individuazione di **aree dedicate e facilmente identificabili**, interne ai locali di P&P Technology;
- utilizzo delle aree esclusivamente per le tipologie di rifiuti ammesse;
- **separazione dei rifiuti per categorie omogenee**, distinguendo rifiuti elettronici e rifiuti urbani;
- divieto di deposito di rifiuti diversi da quelli generati dall'attività di P&P Technology.

I rifiuti sono conservati per il tempo strettamente necessario e comunque fino all'avvio delle operazioni di recupero o smaltimento.

Avvio a recupero o smaltimento

Le operazioni di recupero o smaltimento dei rifiuti urbani sono effettuate secondo le seguenti modalità:

- affidamento esclusivo **ai servizi comunali referenti la sede operativa di P&P Technology**;
- Eventuale avvio a recupero o smaltimento:
  - con periodicità coerente con le esigenze operative di P&P Technology;
  - ovvero al raggiungimento dei limiti quantitativi previsti dalla normativa vigente;
- acquisizione e conservazione della documentazione attestante il corretto smaltimento o recupero dei rifiuti.

Rifiuti Elettronici

In caso di dismissione di attrezzature elettroniche la società P&P Technology procede nel seguente modo.

- Cessione a titolo gratuito, presso enti, scuole laddove ne emerga la necessità e la concreta possibilità di utilizzo
- Cessione a titolo oneroso a fornitori come pezzi di ricambio o scontistica sull'acquisto di nuovi prodotti.

In tutti i casi sopradetti, la società attraverso il proprio ufficio tecnico provvederà alla cancellazione irreversibile dei supporti di registrazione dei dati, tramite operazione di formattazione dei dischi.

Emissioni

Le emissioni derivanti dalle attività di P&P Technology srl sono limitate a quelle tipiche delle normali attività d'ufficio, derivate dall'utilizzo degli impianti di riscaldamento e condizionamento a carico della proprietà dell'immobile e non richiedono autorizzazioni specifiche.

P&P TECHNOLOGY SRL adotta comunque comportamenti organizzativi orientati alla **riduzione dell'impatto ambientale**, quali l'uso razionale delle risorse energetiche e il corretto utilizzo delle apparecchiature.

Protocolli specifici di prevenzione e informative all'OdV

Oltre a quanto espressamente previsto dai precedenti protocolli con riferimento a specifiche Attività Sensibili, i Referenti di P&P Technology srl trasmettono all'OdV le ulteriori informazioni individuate nelle procedure o negli altri Strumenti di attuazione del Modello applicabili, con la periodicità e le modalità previste dagli stessi.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO PREDISPOSTO AI SENSI DEL D.LGS 231/2001

PARTE SPECIALE - 7

RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA

STATO DI REVISIONE DEL DOCUMENTO

Approvato da: Andrea Perpignani, Amministratore Unico____	Data: 02/12/2025

Data revisione :

Descrizione del documento

Ai sensi dell'art. 6 comma 2, lett. a) del D.Lvo 231/01, P&P Technology srl, attraverso un processo di mappatura dei rischi, di valutazione delle attività, dei controlli esistenti e del contesto aziendale in cui opera (cd. *control and risk self assessment)*, ha identificato i processi e le attività *sensibili* (suddivise per tipologia di reato ed elencate nei paragrafi successivi), nell'ambito delle quali possano essere potenzialmente commessi reati tributari previsti dal Decreto.

Per il contrasto al rischio di commissione di tali reati si richiama quanto disposto dal Modello Organizzativo Parte Generale approvato da P&P Technology srl, e tutti i destinatari del Modello sono tenuti ad adottare regole di condotta conformi alla legge, alle disposizioni contenute nel presente documento ed ai principi contenuti nel Codice Etico, al fine di prevenire il verificarsi dei reati tributari previsti dal Decreto.

I principi individuati nel Codice Etico, che qui viene integralmente richiamato costituiscono presupposto e parte integrante dei presidi e delle Misure di controllo descritte nella presenta Parte Speciale con riferimento alle diverse tipologie di destinatari e/o *stakeholders*, nell'ambito delle diverse aree di rischio individuate.

La presente Parte Speciale potrà essere aggiornata dal Presidente o dalla Direzione e tale aggiornamento sarà sottoposto a validazione da parte dell'OdV.

REATO PRESUPPOSTO: art. 25 quinquiesdecies D. Lgs. 231/01

Premessa

L'art. 39, comma 2, Decreto Legge del 26 ottobre 2019, n. 124, recante disposizioni urgenti in materia fiscale e per esigenze indifferibili (legge di conversione definitivamente approvata dal Senato in data 17.12.2019), ha ampliato il novero dei reati-presupposto introducendo nel D. Lgs. 231/01 l'art. 25-quinquiesdecies rubricato "Reati tributari", il quale a sua volta rende concretamente applicabile all'ente, tra le altre misure di cui al D. Lgs. 231 cit., anche la confisca - diretta o per equivalente – del patrimonio dell'ente, nonché il sequestro preventivo di cui all'art. 53 D. Lgs. 231 cit..

La mancata previsione dei tributari nel catalogo dei reati presupposto rendeva infatti possibile che l'autore del reato tributario, privo di disponibilità, riuscisse a sottrarre alla confisca per equivalente beni non direttamente riconducibili al profitto del reato commesso intestandoli alla persona giuridica (si pensi, ad esempio, a beni immobili acquistati mediante il denaro derivante dal "risparmio di spesa" come è quello derivante dal mancato pagamento di un tributo).

La legge di conversione ha dunque aggiunto i reati tributari di cui agli artt. 2 (Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti), 3 (Dichiarazione fraudolenta mediante altri artifici), 8 (Emissione di fatture o altri documenti per operazioni inesistenti), 10 (Occultamento o distruzione di documenti contabili) e 11 (Sottrazione fraudolenta al pagamento di imposte) del D. Lgs. 74/2000.

Fattispecie rilevanti

Sulla base dell'attività condotta da Ente XXX S.r.l., si sono ritenute rilevanti le seguenti fattispecie di reato:

Art. 2 D. Lgs. 74/2000 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti: E' punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni [annuali] relative a dette imposte elementi passivi fittizi. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

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

Il reato in esame punisce all'evidenza l'utilizzo di fatture o altri documenti per operazioni inesistenti finalizzata all'evasione dell'imposta sui redditi o dell'IVA. Come emerge dalla lettura della complessiva disposizione, il reato in questione ha struttura c.d. bifasica poiché si caratterizza da una prima fase di natura propedeutica consistente nell'acquisizione di fatture per operazioni inesistenti (o altra documentazione equipollente) e nella successiva registrazione nelle scritture contabili; e dalla seconda (e necessariamente successiva) fase – in cui concretamente si ha perfezionamento della fattispecie penale - di presentazione della dichiarazione mendace con indicazione degli elementi passivi fittizi riscontrabili nella documentazione falsa acquisita.

La condotta pertanto assume rilevanza penale al momento della presentazione della dichiarazione fiscale (mendace), mentre la sola utilizzazione della documentazione falsa, da intendersi come conservazione o inserimento in contabilità, si configura come ante factum non punibile in quanto meramente strumentale e prodromico alla realizzazione dell'illecito.

Quanto all'oggetto del reato, si precisa che per "altri documenti" diversi dalla fattura debbono intendersi – a mente della definizione di cui all'art. 1 D. Lgs. 74/2000 - quelli aventi rilievo probatorio analogo in base alle norme tributarie; si tratta pertanto di documentazione di natura residuale che tuttavia da un lato, in ottica probatoria nei confronti dell'Amministrazione finanziaria, assolve alla medesima funzione economica della fattura, e dall'altro lato deve essere sempre e comunque "fiscalmente tipica" (nel senso che tutti i documenti che "in base alle norme tributarie" non svolgono una funzione probatoria direttamente in tale ambito, devono ritenersi esclusi). Vedi, ad esempio, la ricevuta fiscale, lo scontrino fiscale, le schede carburanti, le c.d. autofatture, le note di addebito e di credito, i documenti di trasporto, la bolla doganale e così via.

Passando alla responsabilità dell'ente, è abbastanza evidente sia che la commissione di tale reato non possa che essere perpetrata da un soggetto apicale, sia che da una tale condotta illecita l'ente stesso tragga un innegabile vantaggio.

Art. 3 D. Lgs. 74/2000 - Dichiarazione fraudolenta mediante altri artifici: Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte

elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:

a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;

b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

La clausola di riserva che compare in incipit della disposizione rende applicabile la fattispecie in esame a tutte quelle dichiarazioni fraudolente non sanzionate ai sensi dell'art. 2 D. Lgs. 74/2000. Quanto alle peculiari modalità della condotta, si precisa che i "mezzi fraudolenti" (ad es. conti correnti appositamente accesi per le operazioni in nero oppure conti correnti intestati a prestanomi) citati devono essere stati in concreto idonei ad ostacolare l'accertamento fiscale, sia in ambito direttamente tributario, sia in ambito penale.

Si noti infine che questa fattispecie delittuosa può concorrere con quella di cui all'art. 10 D. Lgs. 74/2000, poiché mentre la condotta di cui all'art. 3 in esame è sostanzialmente incentrata sul momento dichiarativo, la condotta di cui all'art. 10 è volta a reprimere le condotte antecedenti il momento dichiarativo potenzialmente preclusive all'accertamento dei redditi.

Art. 8 D. Lgs. 74/2000 - Emissione di fatture o altri documenti per operazioni inesistenti: È punito con la reclusione da quattro a otto anni chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti. Ai fini dell'applicazione della disposizione prevista dal comma 1, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

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

La fattispecie in esame punisce le condotte prodromiche all'evasione, anche laddove queste non abbiano in concreto determinato alcuna evasione di imposta in quanto, ad esempio, il potenziale evasore non abbia fatto alcun uso del documento fiscale. In altre parole, la condotta è punita indipendentemente dall'utilizzo da parte del soggetto ricevente dei documenti falsi.

Tale norma è speculare rispetto all'art. 2 che precede e pertanto si rimanda a tale disposizione ai fini dell'individuazione dell'oggetto materiale della condotta. Si precisa solo che la condotta sanzionata dall'art. 8 è necessariamente commissiva poiché consiste nell'emissione di fatture o nel rilascio di altri documenti relativi ad operazioni inesistenti e di conseguenza la consumazione del reato è da individuarsi nel momento in cui la fattura viene emessa o il documento rilasciato.

Nel caso in esame è infine configurabile anche il tentativo laddove il soggetto attivo abbia già formato la documentazione falsa e questa, poi, non sia stata emessa o rilasciata a terzi per cause indipendenti dalla volontà dell'agente.

Art. 10 D. Lgs. 74/2000 - Occultamento o distruzione di documenti contabili: Salvo che il fatto costituisca più grave reato è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari. La disposizione in esame è volta alla repressione di tutte quelle condotte idonee ad impedire la determinazione dell'esatto ammontare del tributo a prescindere dal fatto che si sia concretamente verificata o meno un'evasione di imposta.

Tale reato (a differenza, ad esempio, delle fattispecie di cui agli artt. 2 e 3 che, benché rivolte a "chiunque" costituiscono reati propri) è un reato comune perché può essere commesso tanto dai soggetti direttamente obbligati alla tenuta delle scritture contabili, quanto da soggetti diversi (si pensi, ad esempio, all'amministratore di fatto di una società).

Presupposto per la sussistenza dell'illecito è infine l'esistenza della documentazione indicata, tra cui non rientrano le c.d. scritture facoltative e cioè quelle istituite per mera comodità e al di fuori di un espresso obbligo di legge.

Art. 11 D. Lgs. 74/2000 - Sottrazione fraudolenta al pagamento di imposte: È punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

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

In questo caso si tratta di un reato proprio e la condotta consiste nell'alienazione simulata o nel compimento di altri atti fraudolenti sui propri o altrui beni, mobili o immobili, posta in essere allo scopo di vanificare in tutto o in parte la procedura di riscossione coattiva attivata in relazione a crediti dell'Erario per le imposte sui redditi o per l'IVA.

L'idoneità della condotta a porre in pericolo il bene protetto dalla norma deve essere valutata con un criterio di prognosi postuma diretto a verificare se al tempo di detta condotta il patrimonio residuo dell'agente fosse o meno sufficiente a rendere efficace la procedura esecutiva. Non vi sarà quindi idoneità laddove i beni residui fossero al momento sufficienti a soddisfare per intero i debiti fiscali.

Non sono dissimili le condotta di cui al comma 2 che tuttavia sanziona la falsa dichiarazione finalizzata al pagamento parziale dei tributi.

Processi Aziendali

I reati previsti dall'art. 25-*quinquiesdecies* e le attività sensibili indicate di seguito impattano sui seguenti processi:

- Amministrazione;
- Contabilità;
- Acquisti.

Attività Sensibili

- attività con soggetti terzi, relative ai rapporti instaurati tra P&P Technology srl e soggetti terzi:
  - contratti di acquisto e/o di vendita con controparti;
  - transazioni finanziarie con controparti;
  - investimenti con controparti; sponsorizzazioni.
- gestione contabile

Procedure e Misure di prevenzione

Aree a rischio

Gestione del processo di sponsorizzazione

Principali funzioni coinvolte: Direzione operativa/generale; Ufficio Contabilità.

Gestione delle risorse finanziarie

gestione dei flussi finanziari (ciclo attivo e ciclo passivo), tesoreria e provvista finanziaria, con particolare riferimento alle seguenti attività: autorizzazione e invio dei pagamenti; inserimento/modifica delle coordinate bancarie del Fornitore.

Principali funzioni coinvolte: Direzione operativa/generale; Contabilità, Consulenti esterni.

Gestione adempimenti societari e fiscali

compilazione, tenuta e conservazione delle scritture contabili rilevanti ai fini fiscali e degli altri documenti di cui è obbligatoria la conservazione;

predisposizione delle dichiarazioni fiscali;

liquidazione delle imposte.

Principali funzioni coinvolte: C.d.A.; Collegio sindacale; Organo di Revisione; Contabilità, Consulenti esterni.

Gestione delle donazioni, delle liberalità e delle attività di fund raising

ricevimento e utilizzo delle donazioni/offerte/liberalità.

Principali funzioni coinvolte: Contabilità.

Principi generali di comportamento

Al fine di evitare il verificarsi dei suddetti reati previsti dal D. Lgs. 231/2001, a tutti i Destinatari, è fatto divieto di:

- ✓ effettuare qualunque tipo di pagamento nell'interesse P&P Technology srl in mancanza di adeguata documentazione di supporto;
- ✓ compiere operazioni che presentino il rischio di essere implicate in vicende relative a riciclaggio di denaro proveniente da attività criminali;
- ✓ utilizzare strumenti anonimi per il compimento di azioni o di operazioni di trasferimento di importi rilevanti;
- ✓ utilizzare contante o altro strumento finanziario al portatore (fermo restando eventuali eccezioni dettate da esigenze operative/gestionali oggettivamente riscontrabili, sempre per importi limitati e comunque rientranti nei limiti di legge) per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie, nonché il divieto di utilizzo di conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia;
- ✓ effettuare versamenti su conti correnti cifrati o presso istituti di credito che non hanno insediamenti fisici in alcun Paese;
- ✓ emettere fatture o rilasciare documenti per operazioni inesistenti al fine di consentire a terzi di commettere un'evasione fiscale;
- ✓ indicare elementi passivi fittizi avvalendosi di fatture o altri documenti aventi rilievo probatorio analogo alle fatture per operazioni inesistenti.

Inoltre, i Destinatari sono tenuti a:

- ✓ astenersi dal porre in essere condotte che, anche solo in astratto o in via potenziale, possano costituire reato ai sensi dell'art. 25-octies del D. Lgs. n. 231/2001;
- ✓ agire nel pieno rispetto della normativa antiriciclaggio e delle procedure interne e di controllo;
- ✓ agire nel rispetto delle procedure adottate e mettere in atto i necessari controlli per la verifica preventiva delle informazioni disponibili sulle controparti commerciali prima di instaurare qualsiasi tipo di rapporto di affari;
- ✓ selezionare i Fornitori sulla base di criteri che prescindono da rapporti personali, favoritismi o altri vantaggi, diversi da quelli dell'esclusivo interesse e beneficio di P&P Technology srl;
- ✓ garantire la regolarità dei pagamenti, con riferimento alla piena coincidenza tra i destinatari dei pagamenti stessi e le controparti effettivamente coinvolte nelle transazioni;
- ✓ effettuare i pagamenti esclusivamente per le attività contrattualmente formalizzate e/o deliberate da P&P Technology srl;
- ✓ garantire che tutte le operazioni e/o transazioni siano autorizzate, correttamente registrate, verificabili, coerenti e congrue;
- ✓ non effettuare registrazioni false, incomplete o ingannevoli e non istituire fondi occulti o non registrati;
- ✓ non utilizzare i fondi e le risorse di P&P Technology srl senza formale autorizzazione;

- ✓ custodire in modo corretto e ordinato le scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali, approntando difese fisiche e/o informatiche che impediscano eventuali atti di distruzione e/o occultamento;
- ✓ verificare l'autenticità e, laddove possibile, la provenienza del denaro contante incassato e utilizzato nell'ambito delle attività di P&P Technology srl ;
- ✓ prestare massima diligenza e attenzione nella gestione del denaro contante al fine di garantire il rispetto della normativa vigente in materia di pagamenti in contanti;
- ✓ non accettare od offrire alcun tipo di donazione, omaggio, regalia o qualsiasi beneficio diretto o indiretto al di fuori dei casi previsti e disciplinati dalle procedure adottate;
- ✓ garantire la tracciabilità del processo di gestione di tutti i prodotti oggetto dell'attività, dall'acquisto all'utilizzo finale;
- ✓ non partecipare al traffico illecito di sostanze stupefacenti.

Protocolli specifici di prevenzione

Gestione delle risorse finanziarie

- ✓ Verifiche, supportate da evidenze formali, atte ad accertare che ogni incasso avvenga nel rispetto di quanto previsto dalla normativa vigente e in modo che sia garantita la tracciabilità di colui che effettua il pagamento, ove possibile (importo, nome/denominazione del soggetto pagatore, causale, indirizzo e numero di conto corrente).
- ✓ Svolgimento di attività di riconciliazione e di conta fisica della cassa. Controllo incrociato tra la stampa della lista cassa e le fatture cartacee emesse dal singolo operatore.
- ✓ Verifiche volte ad accertare le modalità di incasso e/o pagamento, ed in particolare il rispetto del divieto di:
- ✓ trasferire denaro contante quando il valore dell'operazione, anche frazionata, è complessivamente pari o superiore ai limiti di legge;
- ✓ accettare assegni bancari, postali e circolari per importi pari o superiori ai limiti di legge senza la clausola "non trasferibile".

Gestione adempimenti societari e fiscali

Le azioni e le misure da porre in essere per prevenire la commissione del reato di falsa fatturazione presentano alcune peculiarità degne di nota: infatti, diversamente da molte altre fattispecie di reato, i reati tributari sono pervasivi nell'ambito dell'attività di impresa ed è quindi difficile relegarli in ambiti di attività specifici o circoscritti.

La prassi dimostra poi che numerose fattispecie risultano particolarmente insidiose da rilevare, in particolare quando entrano in gioco rapporti con soggetti esteri. Non da ultimo, processi di digitalizzazione non sufficientemente adeguati possono favorire il fenomeno.

La prima linea di difesa per prevenire questa tipologia di reati è l'adozione di un sistema amministrativo – contabile adeguato, che dovrebbe essere affiancato da un sistema gestionale altrettanto efficace. Le "distrazioni" contabili e gestionali, cioè la scarsa attenzione a questi aspetti sono terreno fertile per la commissione dei reati in argomento.

P&P Technology srl da questo punto di vista ha costituito un presidio per la gestione amministrativa consolidato nel tempo.

Si segnala peraltro che il decreto legislativo 14/2019, Codice della crisi d'impresa, già prescrive l'adozione di un adeguato assetto amministrativo-contabile volto a rilevare tempestivamente

eventuali crisi di impresa ad un numero di soggetti addirittura maggiore rispetto a coloro che hanno introdotto i Modelli 231.

Va sottolineato che ai fini della prevenzione del reato di falsa fatturazione non deve essere adottato un assetto amministrativo-contabile ulteriore o nuovo, ma le esigenze e le finalità, pur in apparenza diverse, coincidono per numerosi aspetti.

Può semmai essere sempre valutata l'adozione di qualche funzionalità gestionale e/o contabile ulteriore, ma sempre nell'ambito dell'esistente assetto amministrativo - contabile.

Un buon sistema gestionale e contabile è sicuramente una misura necessaria, ma può non essere sufficiente ai fini di un'efficace prevenzione.

A tal fine si può considerare la possibilità di creare un presidio interno del rischio fiscale.

In linea generale, il presidio del rischio fiscale si estrinseca anzitutto in un preventivo "risk assessment", cioè una valutazione preliminare delle attività e delle aree a maggiore rischio fiscale, nel dotarsi, o nell'individuare tra le risorse esistenti, dall'interno o in outsourcing, di professionalità idonee ad individuare e comprendere i processi e l'organizzazione interni, segnalarne eventuali debolezze e suggerire nel contempo misure correttive, il tutto in un'ottica fiscale.

Da un punto di vista più generale si tratta di rafforzare la corporate governance in ambito fiscale, ovvero di migliorare la tax governance di P&P Technology srl, innervate sulla conoscenza delle principali regole di governo societario sia della materia tributaria.

Procedure di controllo e prevenzione

Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

La presente procedura disciplina le modalità di prevenzione dei reati di cui all'art. 25-octies del D.Lgs. 231/2001 con riferimento a:

- rapporti contrattuali e transazioni con soggetti terzi;
- investimenti e sponsorizzazioni;
- gestione contabile e flussi finanziari.

I principi cardine sono:

- **tracciabilità integrale** delle operazioni;
- **separazione dei ruoli** tra gestione, decisione e controllo;
- **motivazione economica** delle operazioni;
- **divieto di strumenti non tracciabili**.

Ruoli coinvolti

- **Amministrazione Interna (AI)**
  Gestione operativa, registrazioni contabili, raccolta documentale, controlli formali.

- **Amministratore Unico (AU)**
  Autorizzazione delle operazioni rilevanti, valutazione del rischio, gestione delle anomalie.
- **Revisore e Commercialista (RC)**
  Controllo di secondo livello sulla contabilità e sui flussi finanziari, segnalazione criticità.

Rapporti con soggetti terzi e operazioni finanziarie

Avvio e gestione del rapporto

- **AI** acquisisce e conserva dati identificativi della controparte (denominazione, sede, P.IVA/CF, IBAN).
- **AI** verifica la coerenza tra:
  - attività della controparte;
  - oggetto del contratto;
  - valore economico dell'operazione.
- **AU** approva contratti, investimenti e sponsorizzazioni.

Transazioni finanziarie

- Tutti i pagamenti e incassi:
  - avvengono con strumenti **tracciabili**;
  - sono effettuati **esclusivamente** verso/da conti intestati alla controparte contrattuale;
  - riportano causali chiare e coerenti.
- **AI** verifica la documentazione a supporto del pagamento.
- **AU** autorizza le operazioni non ordinarie o di importo rilevante.
- **RC** verifica periodicamente la coerenza dei flussi finanziari.

Investimenti e sponsorizzazioni

- Devono essere **formalizzati per iscritto** e supportati da motivazione economica.
- **AU** valuta preventivamente identità e finalità del beneficiario.
- **AI** conserva la documentazione.
- **RC** verifica la corretta contabilizzazione.

Gestione contabile e controlli

- **AI** registra tutte le operazioni in modo tempestivo e documentato.
- È vietata la registrazione di operazioni fittizie o non giustificate.
- **RC** effettua controlli periodici su:
  - quadrature contabili;
  - flussi finanziari;
  - operazioni atipiche.
- Eventuali anomalie sono segnalate all'**AU**.

Conservazione delle evidenze

Tutta la documentazione relativa a contratti, pagamenti, investimenti e verifiche è conservata in modo ordinato e accessibile, per consentire controlli interni ed esterni.

Check-list Indicatori di Anomalia (art. 25-octies)

La seguente check-list è utilizzata da **AI, AU e RC** come strumento di supporto al controllo.

Operazioni economiche

- Importi sproporzionati rispetto al valore di mercato
- Operazioni prive di chiara motivazione economica
- Investimenti o sponsorizzazioni non coerenti con l'attività aziendale

Pagamenti e flussi finanziari

- Richiesta di pagamento a soggetti diversi dalla controparte contrattuale
- Richiesta di utilizzo di strumenti non tracciabili
- Frazionamento artificioso dei pagamenti
- Causali generiche o poco comprensibili

Comportamenti anomali

- Urgenze ingiustificate nel richiedere pagamenti
- Resistenza a fornire documentazione
- Modifiche improvvise delle modalità di pagamento

Esito

- Nessuna anomalia rilevata
- Anomalia rilevata → attivare procedura di escalation

Protocolli specifici di prevenzione e informative all'OdV

Oltre a quanto espressamente previsto dai precedenti protocolli con riferimento a specifiche Attività Sensibili, i Referenti di P&P Technology srl trasmettono all'OdV le ulteriori informazioni individuate nelle procedure o negli altri Strumenti di attuazione del Modello applicabili, con la periodicità e le modalità previste dagli stessi.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO PREDISPOSTO AI SENSI DEL D.LGS 231/2001

PARTE SPECIALE - 8

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ART. 24-BIS D.LGS. 231/2001)

STATO DI REVISIONE DEL DOCUMENTO

Approvato da: Andrea Perpignani, Amministratore Unico____	Data: 02/12/2025

Data revisione :

Descrizione documento

L'art. 24-bis del D.Lgs. 231/2001 (introdotto dalla L. 18/03/2008 n. 48 e successivamente modificato dai D.Lgs. 7/2016 e 8/2016 e dal D.L. 105/2019) disciplina la responsabilità degli enti per una serie di **reati informatici e di illecito trattamento di dati** commessi nel loro interesse o vantaggio. In generale, i reati ricompresi rappresentano **varie forme di aggressione a sistemi informatici o a dati informatici**. Essi possono distinguersi in due gruppi: da un lato i **reati informatici in senso stretto** (come accessi abusivi o danneggiamenti di sistemi), dall'altro i reati **commessi mediante l'uso di sistemi informatici**, ad esempio falsificazioni di documenti informatici o frodi informatiche legate a firme digitali.

Reati-presupposto ex art. 24-bis. Le fattispecie rilevanti ai fini del D.Lgs. 231/2001 includono, tra le altre:

- **Accesso abusivo a un sistema informatico o telematico** (art. 615-ter c.p.), ossia l'intrusione non autorizzata in sistemi altrui;
- **Detenzione e diffusione abusiva di codici di accesso** a sistemi informatici o telematici (art. 615-quater c.p.);
- **Diffusione di programmi o dispositivi informatici** diretti a danneggiare o interrompere un sistema (art. 615-quinquies c.p.);
- **Intercettazione, impedimento o interruzione illecita** di comunicazioni informatiche o telematiche (art. 617-quater c.p.) e **installazione di apparecchiature per intercettare/impendere** tali comunicazioni (art. 617-quinquies c.p.);
- **Danneggiamento di informazioni, dati e programmi informatici** (art. 635-bis c.p.), compresi quelli **di pubblico interesse** o utilizzati dallo Stato (artt. 635-ter, 635-quater, 635-quinquies c.p.);
- **Falsità in documenti informatici** (art. 491-bis c.p.);
- **Frode informatica del certificatore di firma elettronica** (art. 640-quinquies c.p.);
- **Ostacolo o intralcio ai procedimenti per la sicurezza cibernetica** (art. 1 co.11 D.L. 105/2019, introdotto nell'art. 24-bis).

Rischi e scenari potenziali in azienda

La società in esame è una microimpresa che opera nel settore della formazione, erogando corsi e-learning tramite piattaforma LMS e attività formative in presenza. Alla luce di ciò, sono state individuate due principali **aree di rischio** connesse ai reati informatici e al trattamento dei dati:

- **Attacco alla piattaforma LMS (rischio cyber e privacy):** trattandosi di un sistema centrale nell'operatività aziendale, un attacco informatico all'LMS rappresenta uno scenario critico. La piattaforma gestisce dati personali di utenti/corsisti (nome, cognome, e-mail, codice fiscale, ecc.) memorizzati su server di proprietà dell'ente, ospitati tramite fornitori qualificati con cui esistono contratti di servizio. Un accesso illecito ai sistemi potrebbe comportare la violazione della riservatezza di tali dati (configurando ad esempio accesso abusivo ex art. 615-ter c.p. o diffusione illecita di dati personali) e/o l'alterazione o cancellazione non autorizzata di informazioni didattiche (potenzialmente integrando reati di danneggiamento di dati ex art. 635-bis e ss. c.p.). Considerato il ruolo dell'LMS, eventuali downtime forzati o manomissioni potrebbero paralizzare l'attività formativa online. Questo scenario rileva anche sotto il profilo privacy, costituendo un *data breach* con possibili conseguenze sanzionatorie ai sensi del GDPR, oltre che un reato informatico in senso stretto.

- **Accesso indebito o uso improprio di dati sensibili interni:** la seconda area di rischio riguarda i **dati aziendali riservati e sensibili** (es. documentazione amministrativo contabile, contratti, informazioni su dipendenti e clienti). Tali dati, gestiti esclusivamente dal Responsabile Amministrativo, risiedono in formato digitale all'interno di un ambiente cloud (piattaforma Microsoft) **non sincronizzato su supporti locali**. Un soggetto non autorizzato potrebbe tentare di accedere a queste informazioni riservate violando i sistemi di autenticazione (anche qui configurando ad esempio un reato di accesso abusivo ai sistemi interni). Inoltre, un trattamento illecito o non autorizzato dei dati personali ivi contenuti, ad esempio l'uso difforme da quanto consentito o la divulgazione non autorizzata, costituirebbe una grave violazione delle policy privacy aziendali, potenzialmente rilevante ai fini penali qualora posta in essere con dolo e arrecando nocumento agli interessati. Anche l'ipotesi di sottrazione o dispersione di documenti cartacei contenenti dati sensibili (come contratti o atti amministrativi archiviati) rientra in questo scenario di rischio, sebbene mitigata dalle misure organizzative adottate (archiviazione controllata e accessi limitati).

Misure di prevenzione e controllo adottate

La Società ha implementato specifici **protocolli di sicurezza informatica**, formalizzati in procedure interne, allo scopo di mitigare i rischi sopra evidenziati. Di seguito si riportano le principali misure di prevenzione e controllo in atto:

- **Sicurezza dell'infrastruttura LMS DNA (Distance Network Academy):** l'accesso alla piattaforma (di proprietà dell'Ente) e al server che ospita i dati dei corsisti è consentito solo a personale interno autorizzato, mediante credenziali (username e password) gestite con standard di robustezza e criptazione. Sono in vigore sistemi di protezione e controllo accessi, e viene effettuato un **monitoraggio quotidiano** sugli accessi e di eventuali tentativi anomali di intrusione, sia a cura dell'ente sia da parte dell'unico fornitore tecnologico ammesso. In caso di rilevazione di accessi non autorizzati, sono previste **segnalazioni immediate**: Il provider qualificato notific tempestivamente via telefono o tramite e-mail dedicata (helpdesk@pandpd.it) qualsiasi incidente di sicurezza rilevante. La casella di posta dedicata alle allerte di sicurezza è presidiata quotidianamente da due risorse interne, incaricate di attivare immediatamente le procedure di **incident response** e disaster recovery al bisogno. Questo insieme di misure garantisce tracciabilità degli accessi e pronta gestione degli incidenti, in linea con le best practice organizzative in materia.

- **Protezione dei dati sensibili e policy privacy:** i dati riservati di natura amministrativa e personale sono conservati in formato digitale **su cloud Microsoft** aziendale, senza sincronizzazione su dispositivi locali (ciò riduce il rischio di perdita o furto di dati da computer aziendali). L'accesso a tali archivi cloud è consentito unicamente al Responsabile Amministrativo tramite accesso e autenticazione esclusivamente via web sicura e canali cifrati. Per questa ragione la società ha definito un contratto per la fornitura per tutte le postazioni di una **connessione protetta tramite rete VPN**. Tutti i documenti amministrativi e commerciali sono inoltre gestiti su piattaforme applicative dedicate (fornite da terzi qualificati con regolari contratti di servizio), le quali prevedono misure di sicurezza conformi agli standard di settore. Per la documentazione cartacea (es. copie di contratto, lettere di incarico, registri contabili) vige una rigorosa procedura di archiviazione in aree protette, con accesso limitato alle sole funzioni autorizzate e nello specifico al Responsabile Amministrativo. Sul fronte della privacy, la società aggiorna e attua regolarmente le proprie **policy sul trattamento dei dati personali**, assicurando che ogni trattamento avvenga su basi giuridiche lecite e per scopi determinati, in coerenza con il Regolamento UE 679/2016 (GDPR).

- **Formazione e consapevolezza del personale:** tutto il personale aziendale viene formato periodicamente sulle tematiche di sicurezza informatica e di protezione dei dati. I programmi di formazione interna mirano a diffondere la cultura della **cybersecurity** e le linee guida operative da seguire, istruendo i dipendenti a riconoscere potenziali minacce (es. e-mail di phishing, comportamenti a rischio) e ad adottare le best practice (gestione sicura delle password, utilizzo corretto degli strumenti informatici, rispetto della privacy dei dati trattati). Questa misura è in linea con le raccomandazioni di Confindustria e delle best practice 231, che enfatizzano l'importanza di piani formativi specifici nonché l'adozione di soluzioni tecnologiche come il cloud per migliorare la sicurezza.

Le misure elencate sopra, dalla **tracciabilità degli accessi** alla **separazione dei ruoli e limitazione dei privilegi** sui sistemi critici, fino alla **gestione strutturata delle segnalazioni e degli incidenti**, riflettono un approccio organico alla sicurezza informatica aziendale, volto a minimizzare il rischio di commissione dei reati in esame. Inoltre, l'integrazione tra il modello 231 e le procedure privacy risulta

fondamentale: la società adotta infatti un approccio integrato e coordinato tra le misure previste dal Modello 231 e quelle della propria privacy policy, affinché le due dimensioni (penale-amministrativa e protezione dati) si rafforzino a vicenda. In tal modo viene perseguito il miglior livello possibile di tutela preventiva sia sotto il profilo della responsabilità 231 sia della conformità alla normativa sulla privacy.

Procedure di risposta agli incidenti (accessi anomali, data breach)

La Società ha definito un protocollo di incident response volto a reagire tempestivamente a eventi avversi di natura informatica, come accessi anomali ai sistemi, virus/ransomware o violazioni di dati personali (data breach). Tale protocollo, adeguato alle risorse di una microimpresa, prevede le seguenti fasi principali:

Rilevazione e segnalazione

Attraverso i sistemi di monitoraggio attivi, eventuali attività sospette o non autorizzate vengono individuate il prima possibile. In particolare, la piattaforma LMS e gli altri servizi cloud generano notifiche automatiche in caso di tentativi di accesso falliti ripetuti, accessi da ubicazioni insolite o altre anomalie. Il fornitore tecnico esterno, che supporta l'infrastruttura LMS, effettua un monitoraggio continuo e notifica immediatamente alla Società qualsiasi incidente di sicurezza rilevante, tramite chiamata telefonica diretta o messaggio e-mail verso l'indirizzo dedicato casella helpdesk@pandp.it. Allo stesso modo, ogni dipendente è tenuto a riferire senza indugio al Responsabile Tecnico e all'Amministratore Unico qualsiasi problema informatico grave di cui venga a conoscenza (es. PC infettato da malware, perdita di un device aziendale, sospetto phishing andato a segno). Questo flusso di segnalazioni garantisce l'innesco immediato della procedura di risposta.

Contenimento iniziale

Appena ricevuta una segnalazione di potenziale incidente, il Responsabile Tecnico (con il supporto di eventuali referenti esterni) procede a una rapida verifica dell'evento e adotta le misure di contenimento necessarie. Ciò può includere: disconnessione dalla rete di un dispositivo compromesso; sospensione o blocco temporaneo degli account utente coinvolti in attività anomale; isolamento dei sistemi infetti per evitare la propagazione di malware; modifica urgente delle credenziali compromesse; attivazione delle copie di backup in modalità di sola lettura per preservare i dati. L'obiettivo in questa fase è arrestare o limitare l'impatto dell'incidente, guadagnando tempo per valutazioni più approfondite. Tutte le azioni intraprese vengono tracciate e, se possibile, viene preservata copia dei log e delle evidenze digitali (per eventuali analisi forensi o segnalazioni alle autorità).

Analisi e risposta tecnica

Contenuto il problema, il team di risposta (composto dal Responsabile Tecnico, dall'Amministratore Unico e – se pertinente – dal Responsabile Amministrativo e dal fornitore IT) analizza la natura e la gravità dell'incidente. Vengono identificate le cause (es. vulnerabilità sfruttata, credenziali rubate, errore umano) e valutati i dati/sistemi coinvolti. Sulla base di questa valutazione, si attuano le misure correttive del caso: ad esempio, rimozione del malware e ripristino del sistema operativo pulito;

recupero dei dati dall'ultimo backup integro; applicazione di patch di sicurezza per sanare falle; rafforzamento di firewall o regole di accesso. Se l'incidente riguarda un data breach con fuoriuscita o compromissione di dati personali, la Società attiva parallelamente la procedura prevista dalla normativa privacy, valutando l'obbligo di notifica al Garante per la Protezione dei Dati Personali entro 72 ore e di comunicazione agli interessati, in accordo con gli artt. 33 e 34 GDPR. In ogni caso, l'obiettivo primario è il ripristino della normale operatività in condizioni di sicurezza e la mitigazione di eventuali danni.

Notifica alle autorità competenti

Qualora dall'analisi emerga che l'evento possa configurare un reato informatico (ad es. un accesso abusivo da parte di un estraneo ai sistemi aziendali, una sottrazione dolosa di dati riservati, un sabotaggio informatico) la Società – per il tramite dell'Amministratore Unico – provvede a informare senza ritardo le autorità competenti. In base alla gravità, potrà essere presentata denuncia/querela alle forze dell'ordine fornendo tutte le evidenze raccolte, in modo da permettere l'eventuale perseguimento dei colpevoli. Contestualmente, qualora l'episodio coinvolga dipendenti o collaboratori dell'ente e configuri una violazione interna alle regole del Modello 231, l'Organismo di Vigilanza viene attivato per le opportune verifiche e per l'eventuale avvio di azioni disciplinari.

Recupero e miglioramento

Terminate le azioni di gestione dell'incidente, la fase finale prevede il ripristino completo delle funzionalità e l'implementazione di misure preventive aggiuntive per il futuro. Il Responsabile Tecnico assicura che tutti i sistemi colpiti tornino pienamente operativi (ripristinando i dati da backup, verificando l'integrità delle informazioni e dei servizi). Successivamente, in collaborazione con l'Amministratore Unico, viene condotta una analisi post-incidente per identificare eventuali carenze nei controlli che hanno contribuito all'evento. Sulla base di questa analisi, la Società aggiorna le procedure di sicurezza e rafforza i propri presìdi: ad esempio, può introdurre un controllo aggiuntivo (come l'autenticazione multifattoriale se non presente), intensificare i programmi di formazione mirata per il personale, oppure stipulare contratti aggiuntivi con fornitori specializzati in cyber security. Tutti gli apprendimenti derivanti dall'incidente vengono documentati. L'obiettivo di questa fase conclusiva è trasformare l'accaduto in un'opportunità di miglioramento continuo del sistema di prevenzione.

Procedure per la Gestione delle Violazioni della Privacy

La Società riconosce che una violazione dei dati personali (*data breach*) può costituire, oltre a una violazione della normativa privacy (Reg. UE 679/2016 – GDPR), anche un presupposto di responsabilità ai sensi dell'art. 24-bis del D.Lgs. 231/2001 qualora derivi da accessi abusivi, trattamenti illeciti o danneggiamento di dati informatici.

Al fine di prevenire e gestire correttamente tali eventi, la Società adotta la seguente **procedura operativa di gestione delle violazioni della privacy**, calibrata sulla propria struttura di microimpresa.

Definizione di Violazione dei Dati Personali

Ai fini della presente procedura, costituisce **violazione dei dati personali (data breach)** qualsiasi evento che comporti, anche potenzialmente:

- accesso non autorizzato a dati personali (es. intrusioni informatiche, uso improprio di credenziali);
- perdita o distruzione accidentale di dati (es. cancellazione errata, guasti);
- divulgazione non autorizzata di dati (es. invio errato di documenti, furto di informazioni);
- indisponibilità temporanea o permanente dei dati (es. ransomware, blocco dei sistemi).

La violazione può riguardare dati di clienti/corsisti, dipendenti, collaboratori, fornitori o altri soggetti interessati.

Rilevazione e Segnalazione della Violazione

Tutti i soggetti aziendali (dipendenti, collaboratori, responsabili) sono tenuti a:

- **segnalare immediatamente** qualsiasi evento sospetto o anomalo che possa comportare una violazione di dati personali;
- effettuare la segnalazione senza attendere conferme tecniche definitive.

La segnalazione deve essere indirizzata **senza ritardo** a:

1. **DPO**
2. **RSPP**
3. **Responsabile Tecnico**, e
4. **Amministratore Unico**.

Esempi di eventi da segnalare immediatamente:

- ricezione di alert di sicurezza dai fornitori cloud;
- accessi anomali agli account;
- smarrimento o furto di dispositivi aziendali;
- e-mail inviate per errore con dati personali;
- malfunzionamenti che comportino perdita o blocco dei dati.

Valutazione Iniziale dell'Evento

Il DPO supporta il titolare del trattamento nel:

- verificare se si tratta effettivamente di una **violazione di dati personali**
- analizzare:
    - tipologia di dati coinvolti (comuni, particolari, giudiziari)
    - numero di interessati
    - conseguenze possibili per i diritti e le libertà delle persone

Decisione sulla notifica all'Autorità

Il DPO:

- **consiglia** se la violazione deve essere notificata all'Autorità di controllo (entro **72 ore**)
- collabora alla redazione della notifica verso il **Garante per la protezione dei dati personali**

Ricevuta la segnalazione, il **Responsabile Tecnico**, con il coinvolgimento dell'Amministratore Unico e del Responsabile Amministrativo (se coinvolti dati amministrativi o del personale), procede tempestivamente a:

- identificare la **tipologia di dati coinvolti**;
- verificare se l'evento è ancora in corso;
- stimare l'impatto potenziale sui diritti e le libertà degli interessati;
- valutare se la violazione è riconducibile a:
    - errore umano,
    - carenza organizzativa,
    - attacco informatico,
    - uso improprio dei sistemi.

Tutte le valutazioni vengono documentate in un **registro interno delle violazioni**.

Contenimento e Mitigazione

Qualora venga accertata o anche solo ipotizzata una violazione privacy, la Società adotta immediatamente misure di contenimento, tra cui:

- blocco o sospensione degli account compromessi;
- cambio immediato delle credenziali;
- isolamento dei sistemi coinvolti;
- ripristino dei dati da backup sicuri;
- rimozione di file o accessi non autorizzati;
- coinvolgimento del fornitore tecnologico esterno per supporto tecnico.

L'obiettivo è limitare il più possibile la diffusione, la perdita o l'uso illecito dei dati.

Valutazione degli Obblighi di Notifica

Conclusa la prima fase di analisi, l'Amministratore Unico, con il supporto del Responsabile Tecnico, valuta:

- se la violazione comporta un **rischio per i diritti e le libertà degli interessati**;
- se sussiste l'obbligo di **notifica al Garante per la Protezione dei Dati Personali** entro 72 ore;
- se è necessario informare direttamente gli interessati coinvolti.

In caso di obbligo di notifica:

- la comunicazione viene effettuata in modo tempestivo, completo e documentato;
- viene conservata evidenza delle comunicazioni effettuate.

Coinvolgimento del Modello 231 e dell'OdV

Qualora la violazione privacy:

- sia riconducibile a comportamenti dolosi o gravemente negligenti,
- integri ipotesi di accesso abusivo, trattamento illecito o danneggiamento di dati,
- evidenzi carenze organizzative rilevanti,

l'Amministratore Unico informa tempestivamente l'**Organismo di Vigilanza (OdV)** affinché:

- valuti la rilevanza dell'evento ai fini del D.Lgs. 231/2001;
- verifichi l'adeguatezza delle procedure in essere;
- proponga eventuali misure correttive o disciplinari.

Documentazione e Miglioramento Continuo

Ogni violazione, anche se non soggetta a notifica esterna, viene:

- documentata in un **registro interno dei data breach**;
- analizzata per individuare cause e responsabilità;
- utilizzata come base per aggiornare:
    - procedure interne,
    - misure di sicurezza,
    - attività formative.

La Società considera la gestione delle violazioni privacy parte integrante del sistema di prevenzione dei reati informatici e del trattamento illecito dei dati.

Valutazione del rischio residuo

Alla luce dei controlli implementati, la **esposizione residua al rischio** per questa categoria di reati è valutata come **lieve**. La microimpresa, pur facendo ampio uso di strumenti informatici per la propria attività, ha **formalizzato protocolli di sicurezza** e predisposto difese che riducono significativamente le opportunità di condotte illecite informatiche. Nonostante tutto ciò, nella matrice di rischio aziendale il rischio di commissione di *delitti informatici* risulta attualmente classificato come **Alto,** considerando che i dati più recenti indicano che gli attacchi informatici gravi sono in forte crescita a livello globale e questa tendenza mostra che il fenomeno è in espansione costante e non episodica. Diversi fattori supportano questa prudenza

- Crescente gravità e impatto:

- Sofisticazione delle tecniche di attacco:
- Superficie di attacco in espansione:
- Minacce in rapida evoluzione e imprevedibili.

Per questa ragione la direzione mantiene alta l'attenzione su questi temi e si impegna a riesaminare periodicamente il rischio **cyber** e di trattamento dati, adeguando all'occorrenza le misure organizzative e tecniche per garantire un livello di sicurezza sempre in linea con le **migliori pratiche** e con la normativa vigente.

Protocolli specifici di prevenzione e informative all'OdV

Oltre a quanto espressamente previsto dai precedenti protocolli con riferimento a specifiche Attività Sensibili, i Referenti di P&P Technology srl trasmettono all'OdV le ulteriori informazioni individuate nelle procedure o negli altri Strumenti di attuazione del Modello applicabili, con la periodicità e le modalità previste dagli stessi.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO PREDISPOSTO AI SENSI DEL D.LGS 231/2001

PARTE SPECIALE - 9

REATI IN MATERIA DI WHISTLEBLOWING

STATO DI REVISIONE DEL DOCUMENTO

Approvato da: Andrea Perpignani, Amministratore Unico____	Data: 02/12/2025

Data revisione :

Descrizione del Documento

La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo (di seguito "Modello 231" o "MOG") è redatta in conformità all'art. 6 del Decreto Legislativo 8 giugno 2001, n. 231 e successive modificazioni. Tale documento integra il Modello 231 di P&P Technology srl con specifico riferimento ai reati e illeciti riconducibili al whistleblowing, ossia alle condotte illecite inerenti la gestione delle segnalazioni di violazioni e alla tutela dei segnalanti. Essa costituisce parte integrante del sistema di controllo interno della Società e definisce principi, protocolli e misure volti a prevenire il rischio di comportamenti che possano configurare violazioni delle normative in materia di whistleblowing.

In linea con i requisiti di legge, questa Parte Speciale descrive le attività sensibili e i processi aziendali interessati, nonché le regole di condotta e le misure di prevenzione che la Società – P&P Technology srl, microimpresa operante nel settore della formazione – adotta per prevenire eventuali atti illeciti o irregolarità connesse alle segnalazioni interne.

La presente Parte Speciale potrà essere aggiornata dal Presidente o dalla Direzione e tale aggiornamento sarà sottoposto a validazione da parte dell'OdV.

Reato Presupposto e Normativa di Riferimento

In questa sezione si individuano i reati presupposto rilevanti in materia di whistleblowing e si richiamano le principali normative vigenti applicabili. Benché il fenomeno del whistleblowing sia disciplinato soprattutto da norme di carattere amministrativo e giuslavoristico, ai fini del Modello 231 esso assume rilievo in quanto parte integrante dei presidi organizzativi richiesti per l'esonero di responsabilità dell'ente.

Le fattispecie di illecito rilevanti ai fini della presente Parte Speciale includono in particolare:

- Atti di ritorsione o discriminatori contro il segnalante, commessi in ragione di una segnalazione effettuata (es. licenziamento, demansionamento, molestie, ostracismo). Tali comportamenti sono vietati e sanzionati dalla legge e devono considerarsi nulli e privi di effetto;
- Ostacolo o tentativo di ostacolo all'inoltro o alla gestione di una segnalazione, ad esempio impedendo o ritardando il flusso delle informazioni, o interferendo sulle attività di verifica;
- Violazione dell'obbligo di riservatezza circa l'identità del segnalante (o di altri soggetti menzionati nella segnalazione), divulgando informazioni riservate che possano consentire l'identificazione non autorizzata;
- Omissione nell'istituzione del canale di segnalazione o nella sua gestione secondo i requisiti di legge (mancata attivazione del canale interno, mancata adozione di procedure adeguate, omessa verifica e analisi delle segnalazioni ricevute).

Sebbene i comportamenti sopra elencati non configurino attualmente reati penali autonomi contemplati nel catalogo del D.Lgs. 231/2001, il Decreto Legislativo 10 marzo 2023, n. 24 (di seguito "D.Lgs. 24/2023" o "Decreto Whistleblowing") ha introdotto importanti obblighi legali per gli enti in materia di protezione dei segnalanti. In particolare, l'art. 21 del D.Lgs. 24/2023 prevede sanzioni amministrative pecuniarie fino a 50.000 euro a carico dell'ente nel caso in cui vengano accertati atti di ritorsione, ostacoli alle segnalazioni, violazioni della riservatezza, oppure la mancata istituzione di canali e procedure adeguate alle segnalazioni.

Tali sanzioni sono irrogate dall'Autorità Nazionale Anticorruzione (ANAC) a seguito di istruttoria e accertamento, e hanno un significativo effetto deterrente.

Le principali fonti normative di riferimento per questa Parte Speciale sono di seguito elencate:

- D.Lgs. 8 giugno 2001, n. 231, art. 6, commi 2-bis, 2-ter e 2-quater: disposizioni che richiedono agli enti dotati di Modello 231 l'adozione di canali di segnalazione idonei a garantire la riservatezza del segnalante, nonché l'introduzione di misure disciplinari per sanzionare eventuali violazioni di tali obblighi o segnalazioni infondate in mala fede. Tali previsioni, inizialmente introdotte dalla Legge 179/2017, sono state riviste e rafforzate dal D.Lgs. 24/2023;
- D.Lgs. 10 marzo 2023, n. 24 – Attuazione della Direttiva (UE) 2019/1937 in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e disposizioni in materia di segnalazioni di violazioni delle disposizioni normative nazionali: normativa di riferimento sul whistleblowing in Italia, applicabile al settore privato e pubblico, che impone l'istituzione di sistemi di segnalazione interni ed esterni e rafforza la tutela del segnalante. Per le società dotate di Modello 231 (anche con meno di 50 dipendenti), il decreto impone l'adeguamento dei canali di segnalazione ai nuovi requisiti e amplia la platea dei soggetti tutelati;
- Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio, relativa alla protezione degli informatori (EU Whistleblowing Directive), recepita in Italia dal D.Lgs. 24/2023, cui il legislatore nazionale si è conformato nel definire standard minimi di tutela e obblighi per gli enti;
- Normativa giuslavoristica e di tutela del lavoratore: in particolare la Legge 20 maggio 1970 n. 300, art. 2 (Statuto dei Lavoratori) e la Legge 15 luglio 1966 n. 604 in materia di licenziamenti, come modificate dal D.Lgs. 24/2023, che sanciscono la nullità di eventuali provvedimenti disciplinari o di licenziamento ritorsivi adottati a causa di una segnalazione; nonché le disposizioni in materia di tutela della riservatezza dei dati personali (GDPR UE 2016/679 e D.Lgs. 196/2003 s.m.i.) applicabili al trattamento dei dati nelle segnalazioni.

È opportuno precisare che il campo di applicazione oggettivo di questa Parte Speciale, per le imprese di piccole dimensioni come la nostra, riguarda principalmente le violazioni del Modello 231 e gli illeciti rilevanti ai sensi del D.Lgs. 231/2001. In base al D.Lgs. 24/2023, infatti, per gli enti di diritto privato che hanno adottato un Modello 231 ma non raggiungono la soglia dimensionale dei 50 dipendenti, l'obbligo di attivare un canale di whistleblowing sussiste con riferimento esclusivo alle violazioni delle norme nazionali e dei reati presupposto che il Modello intende prevenire. Ciò significa che, nel contesto della presente microimpresa, le segnalazioni gestite attraverso il canale interno riguarderanno in via principale: (i) comportamenti o eventi che possano integrare reati presupposto ex D.Lgs. 231/2001 o violazioni del Modello 231 aziendale, e (ii) altri illeciti che possano ledere l'interesse pubblico o l'integrità dell'ente nell'ambito dell'attività aziendale. Resta ferma la possibilità, per i segnalanti, di rivolgersi ai canali esterni (ANAC o autorità competenti) nei casi previsti dalla legge, ad esempio qualora il canale interno non sia istituito o non funzioni adeguatamente.

Premessa: Rischio Whistleblowing

Premessa Generale. La Società P&P Technology srl, pur essendo una microimpresa operante nel settore della formazione, riconosce l'importanza cruciale di un efficace sistema di whistleblowing quale strumento di emersione precoce di comportamenti illeciti o irregolari e quale presidio a tutela dell'etica aziendale e della legalità. Il rischio connesso al whistleblowing non va inteso come il rischio di segnalazioni in sé, bensì come il rischio di gestione scorretta delle segnalazioni o di adozione di comportamenti repressivi che possano esporre la Società a sanzioni o pregiudizi reputazionali. In altre parole, il rischio rilevante è che la Società (attraverso i propri esponenti, dipendenti o collaboratori) ometta di prevenire o gestire adeguatamente le segnalazioni di illeciti, oppure ponga in

essere azioni contrarie alla tutela del segnalante, incorrendo così nelle violazioni delineate al paragrafo precedente.

Applicabilità del Modello 231 e obblighi ex lege. L'adozione volontaria del Modello 231 da parte della Società implica l'assunzione di specifici obblighi organizzativi in materia di whistleblowing. Ai sensi del D.Lgs. 24/2023, infatti, anche le imprese con meno di 50 dipendenti che abbiano adottato un Modello 231 sono tenute a dotarsi di un canale interno di segnalazione conforme ai requisiti di legge. Ciò conferma la rilevanza del sistema di whistleblowing anche in contesti aziendali di piccole dimensioni: l'efficace funzionamento del canale di segnalazione interno viene ora considerato elemento essenziale dell'idoneità del Modello 231 e sarà valutato dall'Autorità giudiziaria nell'eventuale verifica dell'effettiva attuazione del Modello stesso. In altri termini, un modello di organizzazione che non includa un adeguato sistema di whistleblowing non può ritenersi efficace e potrebbe pregiudicare la posizione dell'ente in sede di accertamento giudiziale.

Rilevanza del rischio whistleblowing nel settore formazione. La Società opera nel campo della formazione e consulenza, un settore nel quale le possibilità di commissione di reati presupposto D.Lgs. 231/2001 possono essere più limitate rispetto ad industrie di maggiori dimensioni o operanti in settori altamente regolamentati. Tuttavia, anche nell'ambito delle attività formative esistono potenziali aree di rischio che rendono necessario un sistema di segnalazione interno efficace. Ad esempio, nell'erogazione dei servizi formativi potrebbero verificarsi irregolarità amministrative, contabili o fiscali; ovvero, la Società potrebbe trovarsi coinvolta in progetti finanziati da enti pubblici o fondi europei, ambito in cui eventuali condotte illecite (es. frodi nelle pubbliche forniture, malversazioni) avrebbero l'obbligo di essere prontamente intercettate e affrontate tramite segnalazione interna. Inoltre, la tutela del patrimonio informativo e reputazionale dell'azienda nel settore formazione è fondamentale: una segnalazione gestita in modo inadeguato – ad esempio ignorata fino a sfociare in una denuncia pubblica – potrebbe causare gravi danni reputazionali. Pertanto, la Società considera la prevenzione del rischio whistleblowing una parte integrante del proprio sistema di controllo.

Commitment aziendale. La Società ha già manifestato il proprio impegno su questi temi adottando un Regolamento interno per la gestione delle segnalazioni, pubblicato sul sito web aziendale e messo a disposizione di tutti i Destinatari. Tale regolamento – coerente con le previsioni del D.Lgs. 24/2023 – disciplina dettagliatamente le modalità con cui possono essere effettuate e gestite le segnalazioni, i soggetti coinvolti, nonché le tutele garantite al segnalante. La presenza di un Organismo di Vigilanza (OdV) attivo fin dalla data di adozione del Modello 231 testimonia inoltre la volontà della Società di vigilare costantemente sull'efficacia e sull'osservanza del sistema di whistleblowing. Il presente documento consolida e integra tali misure, fornendo un riferimento organico e ufficiale in seno al Modello 231.

Mappatura dei Processi Aziendali Coinvolti

Alla luce dell'analisi del rischio condotta, sono stati individuati i processi aziendali maggiormente coinvolti o sensibili in relazione al rischio whistleblowing. La mappatura di tali processi è funzionale a concentrare i presidi di controllo nelle aree dove è più probabile o più impattante l'eventuale occorrenza di condotte illecite o irregolari connesse alla gestione delle segnalazioni. Di seguito si elencano i principali processi rilevanti per la presente Parte Speciale:

- Processo di Segnalazione Interna e Gestione delle Segnalazioni: include tutte le fasi dalla ricezione della segnalazione da parte del segnalante, alla protocollazione e presa in carico, fino all'istruttoria interna, conclusione delle verifiche e eventuale risposta al segnalante. Questo processo costituisce il fulcro del sistema whistleblowing e coinvolge il canale di

segnalazione dedicato (piattaforma informatica, indirizzo email dedicato, linea telefonica, etc.) e i soggetti/delegati preposti alla gestione delle segnalazioni;

- Processo di Investigazione Interna e Adozione di Misure Conseguenti: consiste nell'attività di verifica e approfondimento delle segnalazioni ricevute. Può coinvolgere, di volta in volta, funzioni aziendali di controllo (ad es. funzioni di Compliance, Internal Audit, Responsabile Legale, HR) o consulenti esterni incaricati, sotto il coordinamento dell'OdV o del gestore del canale. Comprende anche l'attuazione di eventuali provvedimenti correttivi o sanzionatori a seguito dell'accertamento di violazioni segnalate;
- Processo di Gestione del Personale e delle Relazioni di Lavoro: comprende le attività di amministrazione del personale, valutazione delle performance, promozioni, mobilità, provvedimenti disciplinari e cessazioni del rapporto di lavoro. Questo processo è rilevante in ottica whistleblowing poiché eventuali atti ritorsivi o discriminatori verso il segnalante si manifestano tipicamente attraverso decisioni attinenti al rapporto di lavoro (es. licenziamento, mancata promozione, trasferimento ingiustificato, modifica peggiorativa delle mansioni o dell'orario). È pertanto necessario presidiare tali attività per garantire che ogni decisione sia assunta su basi oggettive e non in conseguenza di una segnalazione effettuata;
- Processo di Monitoraggio e Controllo da parte dell'OdV: riguarda l'insieme delle attività attraverso cui l'Organismo di Vigilanza vigila sull'effettiva implementazione e sul funzionamento del sistema di segnalazione. Include, ad esempio, la verifica periodica del corretto funzionamento del canale interno (anche attraverso accessi al sistema informatico dedicato), l'analisi delle segnalazioni pervenute e dell'esito delle relative istruttorie, nonché il coordinamento con le altre funzioni aziendali di controllo (se presenti) e la predisposizione di report periodici all'organo amministrativo sui risultati del monitoraggio.

Ognuno dei suddetti processi presenta potenziali criticità specifiche, descritte nella successiva sezione sulle Attività Sensibili, che potrebbero esporre la Società al rischio di violare le normative sul whistleblowing. La presente mappatura consente di stabilire con chiarezza "chi fa cosa" nell'ambito della gestione delle segnalazioni e di individuare punti di controllo appropriati in ciascun processo.

Attività Sensibili e Potenziali Modalità Attuative delle Violazioni

All'interno dei processi mappati, si definiscono di seguito le Attività Sensibili, ovvero quelle specifiche fasi o operazioni nelle quali si concentra il rischio di comportamenti non conformi alle disposizioni di legge o ai principi del Modello 231 in materia di whistleblowing. Per ciascuna attività sensibile vengono anche evidenziate, in via esemplificativa, le possibili modalità attraverso cui potrebbe concretizzarsi una violazione o un aggiramento delle regole. L'individuazione di tali attività consente di tarare misure di prevenzione mirate e proporzionate alla dimensione aziendale.

- Ricezione e Registrazione delle Segnalazioni: fase in cui una comunicazione riservata viene inviata dal segnalante tramite i canali predisposti (es. piattaforma online, e-mail dedicata, linea telefonica, colloquio diretto). Rischi: mancata registrazione della segnalazione (es. omessa protocollazione deliberata per occultare la segnalazione); divulgazione non autorizzata dell'esistenza o del contenuto della segnalazione a persone non autorizzate (violando la riservatezza); rifiuto o ostruzionismo nel ricevere la segnalazione (ad esempio scoraggiare il segnalante dal formalizzare la segnalazione, o chiudere il canale in modo da renderlo inutilizzabile).
- Valutazione di Ammissibilità e Istruttoria Preliminare: comprende il primo esame della segnalazione ricevuta per determinarne l'oggetto, la plausibilità e le modalità di gestione (es. assegnazione a un referente investigativo, archiviazione se manifestamente infondata

o priva di elementi). Rischi: valutazione arbitraria o negligente che porti a scartare indebitamente segnalazioni fondate (es. insabbiamento di una segnalazione riguardante un apicale); mancata attivazione dell'indagine interna per conflitto di interessi o connivenza; omessa tempestività nell'avviare gli accertamenti necessari, consentendo che il comportamento illecito segnalato prosegua indisturbato.

- Indagine Interna e Raccolta di Evidenze: comprende tutte le attività svolte per verificare i fatti oggetto di segnalazione (colloqui con le persone coinvolte, analisi documentale, audit tecnici, ecc.). Rischi: conduzione inadeguata o parziale dell'indagine al fine di minimizzare o non far emergere le responsabilità (es. l'addetto all'indagine è subordinato o vicino al soggetto segnalato e tende a sminuire i fatti); violazione della riservatezza durante l'indagine (es. divulgazione dell'identità del segnalante o del contenuto della segnalazione oltre il ristretto team autorizzato); mancata tracciabilità delle attività svolte e delle risultanze, rendendo difficile successive verifiche da parte dell'OdV o delle autorità.
- Reporting dell'Esito e Azioni Correttive: fase finale in cui si formalizza l'esito delle verifiche (ad esempio redigendo una relazione interna) e si intraprendono eventuali azioni conseguenti. Rischi: omessa comunicazione dell'esito al segnalante nei termini previsti, ledendo il suo diritto ad un riscontro; mancata segnalazione all'autorità esterna competente in presenza di violazioni gravi ove ciò sia obbligatorio (es. mancata denuncia all'Autorità giudiziaria nonostante evidenze di reato emerse dall'indagine interna); omessa adozione di provvedimenti disciplinari o correttivi verso gli autori delle violazioni accertate (lasciando impunite le condotte illecite segnalate); adozione, per converso, di provvedimenti punitivi o ritorsivi verso il segnalante invece che verso il responsabile della violazione.
- Decisioni sul Personale riguardanti il Segnalante: qualsiasi atto gestionale che coinvolga il segnalante in seguito a una segnalazione (come note di demerito, valutazioni negative, esclusione da progetti, revoca di opportunità di formazione, modifica dell'orario o delle mansioni). Rischi: ritorsioni o discriminazioni motivate dalla segnalazione effettuata, mascherate da normali decisioni organizzative. Ad esempio: assegnare al segnalante mansioni inferiori o trasferirlo ingiustificatamente (demansionamento); interrompere un contratto a termine o non procedere a un previsto rinnovo/assunzione a tempo indeterminato altrimenti atteso; isolamento del segnalante nell'ambiente di lavoro (ostracismo) o molestie sottili; diminuzione immotivata della retribuzione o delle opportunità di carriera. Tali atti, oltre a costituire violazione di legge, comprometterebbero la fiducia nel sistema di segnalazione, inducendo altri dipendenti a non segnalare per timore di subire analoghe conseguenze.
- Gestione delle Informazioni e Documentazione delle Segnalazioni: comprende la conservazione, archiviazione e protezione dei dati relativi alle segnalazioni (identità del segnalante, documenti raccolti, report investigativi). Rischi: conservazione non sicura dei documenti, con possibili accessi non autorizzati; mancata cancellazione dei dati decorso il periodo previsto (5 anni dall'esito finale, come indicato dalla normativa), con conseguente violazione delle norme privacy; difetto di segregazione dei ruoli che permetta a personale non autorizzato di consultare dettagli sulle segnalazioni.
- Segnalazioni infondate e in mala fede

Procedure e Misure di Prevenzione

Alla luce delle attività sensibili individuate, la Società adotta un insieme strutturato di procedure di controllo e misure di prevenzione finalizzati a mitigare il rischio di commissione delle violazioni in materia di whistleblowing. Tali misure, pur calibrate sulla realtà di una microimpresa, rispettano i

principi di legalità, riservatezza e tutela del segnalante, in coerenza con le normative vigenti e le migliori prassi. Di seguito si illustrano i principali protocolli e presìdi implementati:

Istituzione di Canali di Segnalazione Interni Conformi

Sono attivi tre diversi canali dedicati alla raccolta delle segnalazioni, idonei a garantire la riservatezza dell'identità del segnalante e delle persone coinvolte. In particolare, la Società ha istituito

- Forma scritta tramite l'indirizzo e-mail odv.pandp@gmail.com
- Incontro riservato
- Segnalazione in forma scritta tramite raccomandata/posta ordinaria.

In tutti i casi potrà richiedere un incontro diretto con il gestore delle segnalazioni, nella persona del presidente dell'Organo di Vigilanza. Tali modalità multiple assicurano che il segnalante possa scegliere lo strumento a sé più congeniale e che nessuna segnalazione venga impedita per ragioni tecniche. Le istruzioni per accedere ai canali e per effettuare una segnalazione sono dettagliate nel Regolamento aziendale sulle segnalazioni e comunicate a tutto il personale e rese pubbliche in una sezione dedicata "Trasparenza e Compliance" presente sul sito internet aziendale all'indirizzo www.pandp.it .

Nomina del Gestore del Canale e Procedure di Gestione

La Società ha formalmente individuato il gestore del canale interno di segnalazione, figura dotata dei requisiti di autonomia e competenza necessari. Nel nostro caso, data la dimensione aziendale, la funzione di gestore del canale è affidata all'Organismo di Vigilanza (OdV) in composizione monocratica (ovvero al membro OdV designato, in caso di OdV collegiale): tale scelta è ritenuta idonea in quanto l'OdV è un organo indipendente e competente in materia di controllo ex D.Lgs. 231. Il gestore del canale/OdV opera secondo una Procedura interna per la gestione delle segnalazioni (allegata al Modello 231), che disciplina in dettaglio ogni fase: ricezione, registrazione, filtro preliminare, istruttoria, relazione conclusiva e archiviazione. La procedura definisce tempistiche chiare (in linea con il termine di riscontro di 3 mesi previsto dalla normativa), modalità di comunicazione dell'esito al segnalante e criteri di coinvolgimento, se necessario, di altre funzioni aziendali o consulenti esterni per l'istruttoria. Tutte le attività svolte vengono adeguatamente tracciate e documentate al fine di consentire verifiche successive e di fornire evidenza dell'osservanza delle regole.

Misure di Tutela della Riservatezza

Vengono adottate misure tecniche e organizzative rigorose per garantire che l'identità del segnalante, nonché il contenuto delle segnalazioni e l'identità degli eventuali soggetti menzionati, restino confidenziali in tutte le fasi. L'accesso alle segnalazioni è riservato esclusivamente al gestore del canale e ai soggetti espressamente autorizzati dall'OdV a svolgere attività istruttoria sul caso concreto. I documenti e i file inerenti alle segnalazioni sono conservati in un archivio riservato all'OdV. La normativa vigente (GDPR e D.Lgs. 24/2023) viene rispettata anche in termini di data retention: le segnalazioni e la documentazione correlata vengono cancellate trascorsi 5 anni dalla conclusione del procedimento di segnalazione, salvo che siano in corso ulteriori obblighi di conservazione (ad es. per supportare investigazioni dell'autorità). Eventuali richieste di accesso a informazioni relative a segnalazioni (es. istanze di accesso agli atti) vengono gestite dall'OdV caso per

caso, applicando le esclusioni di legge in materia di accesso e valutando soluzioni come l'oscuramento di dati identificativi per tutelare la confidenzialità.

Divieto di Ritorsione e Misure Antidiscriminatorie

La Società adotta una politica di tolleranza zero verso qualsiasi forma di ritorsione o discriminazione ai danni del segnalante. Tale principio è esplicitato nel Codice Etico e nel Regolamento whistleblowing ed è portato a conoscenza di tutti i Destinatari. In concreto, è fatto divieto a qualunque livello gerarchico di influenzare negativamente la posizione lavorativa del segnalante in ragione della segnalazione effettuata. Ogni decisione concernente il segnalante (provvedimenti disciplinari, cambiamenti di mansione, trasferimenti, progressioni di carriera, accesso a opportunità formative, ecc.) adottata entro un determinato periodo successivo alla segnalazione è soggetta a particolare scrutinio: il gestore del canale e/o l'OdV, in collaborazione con il responsabile dell'ente formativo, che riveste anche il ruolo di Amministratore Unico della società P&P Technology srl verificano la sussistenza di ragioni oggettive e documentate a supporto di tali decisioni, al fine di escludere motivazioni ritorsive. Inoltre, come ulteriore presidio, il segnalante ha la facoltà di rivolgersi direttamente all'OdV per segnalare eventuali atti che ritenga ritorsivi subiti dopo la propria segnalazione, indipendentemente dagli ordinari canali di HR, così che l'OdV possa esaminare il caso ed eventualmente attivare la procedura prevista dall'art. 21 del D.Lgs. 24/2023 (segnalazione all'ANAC dell'avvenuta ritorsione). La Società si impegna espressamente a garantire che, laddove un segnalante provi di aver effettuato una segnalazione ai sensi di legge e di aver subito in seguito un trattamento pregiudizievole, ricadrà sul datore di lavoro l'onere di provare che tali misure sono motivate da ragioni estranee alla segnalazione, in conformità con il regime probatorio delineato dalla normativa vigente. Tale impegno ha anche finalità dissuasive interne: rende chiaro che ogni potenziale responsabile di condotte ritorsive sarà chiamato a rispondere del proprio operato.

Formazione e Sensibilizzazione

Lla Società investe sulla formazione del personale in materia di whistleblowing. Attraverso sessioni formative periodiche (inserite eventualmente in programmi più ampi di formazione sulla compliance e sul Modello 231) e comunicazioni interne mirate, i dipendenti e collaboratori vengono informati circa: l'esistenza e le finalità del canale di segnalazione; le modalità operative per effettuare segnalazioni tutelate; i diritti e le tutele garantite dalla legge (in particolare l'assenza di conseguenze disciplinari o contrattuali ingiustificate per chi segnala in buona fede); e i doveri di ciascuno in caso di coinvolgimento in un procedimento di segnalazione (es. collaborare alle indagini interne, mantenere la riservatezza, ecc.).

Misure Disciplinari e Conseguenze in caso di Violazioni

In ottemperanza a quanto richiesto dall'art. 6 del D.Lgs. 231/2001 e dall'art. 21, comma 2, del D.Lgs. 24/2023, la Società ha integrato il proprio sistema disciplinare prevedendo specifiche sanzioni interne verso: (i) chiunque realizzi comportamenti di natura ritorsiva o comunque violi le misure di protezione del segnalante o la riservatezza dovuta (dirigenti, preposti o dipendenti che siano); nonché (ii) eventuali segnalanti che con dolo o colpa grave effettuino segnalazioni infondate in mala fede. In particolare, il divieto di ritorsione verso i segnalanti è oggetto di una clausola specifica nel Codice Disciplinare aziendale: la violazione di tale divieto costituisce infrazione di massima gravità, passibile delle sanzioni più severe (fino al licenziamento per giusta causa, se commessa da un dipendente). Parimenti, la violazione dell'obbligo di riservatezza sul caso e sull'identità del segnalante configura grave inadempimento disciplinare. Quanto agli abusi del canale da parte di segnalanti in mala fede

(ad esempio segnalazioni volutamente false o diffamatorie), essi comportano la perdita delle tutele legali per il segnalante e possono dar luogo a provvedimenti disciplinari appropriati, nel rispetto di quanto previsto dal Contratto Collettivo Nazionale di Lavoro (CCNL) applicabile e dallo Statuto dei Lavoratori. L'apparato sanzionatorio interno è dunque calibrato per sanzionare sia la mancata osservanza delle procedure di whistleblowing sia i comportamenti ostativi o scorretti, in modo da assicurare l'effettività del sistema. Inoltre, l'OdV vigila affinché in tutti i casi di accertata violazione delle regole sul whistleblowing vengano attivate senza indugio le conseguenti azioni disciplinari, segnalando all'Organo Direttivo eventuali inerzie o omissioni in tal senso.

Flusso Informativo verso l'Organismo di Vigilanza (OdV)

Un adeguato flusso informativo nei confronti dell'Organismo di Vigilanza è essenziale per garantire l'efficacia del sistema di controllo ex D.Lgs. 231/2001. In materia di whistleblowing, la Società definisce il seguente flusso informativo verso l'OdV, nel rispetto dei principi di autonomia e indipendenza di tale organo:

- Comunicazione delle Segnalazioni Ricevute: l'OdV deve essere tempestivamente informato di ogni segnalazione inerente violazioni rilevanti ai fini del Modello 231. Nel caso in cui l'OdV stesso non coincida con il gestore del canale di segnalazione, quest'ultimo ha l'obbligo di trasmettere all'OdV, senza ritardo, copia (o estratto) di tutte le segnalazioni che riguardino presunte violazioni del Modello 231, reati presupposto o comunque fatti di gravità tale da poter compromettere l'integrità dell'ente. Le modalità di trasmissione all'OdV garantiscono la tutela della riservatezza (ad es. inviando le informazioni prive di dati identificativi non necessari, se non già noti all'OdV in quanto gestore). Qualora la segnalazione riguardi direttamente membri dell'OdV o ambiti di competenza dell'OdV stesso, è previsto che essa sia gestita da un membro alternativo o da un organo di controllo equivalente per assicurare l'imparzialità, informandone comunque l'OdV istituzionale.
- Accesso alla Documentazione e Audit dell'OdV: l'OdV ha in ogni momento pieno accesso alla documentazione relativa alle segnalazioni trattate, inclusi i report di indagine, i verbali e gli atti dei procedimenti disciplinari eventualmente avviati. A tal fine, tutti i documenti sulle segnalazioni sono archiviati in modo organizzato e accessibile all'OdV, pur nel rispetto dei vincoli di riservatezza. L'OdV può effettuare periodicamente verifiche a campione sul processo di gestione delle segnalazioni, controllando ad esempio che ogni segnalazione sia stata gestita secondo la procedura, che i tempi di risposta siano stati rispettati e che le misure di tutela siano state applicate correttamente. Gli esiti di tali verifiche vengono riportati dall'OdV nelle proprie relazioni all'Organo Amministrativo.
- Segnalazione all'Organo Amministrativo e alle Autorità: l'OdV, nell'ambito del suo dovere di vigilanza, qualora rilevi significative carenze o violazioni nel sistema di whistleblowing (ad es. mancata attuazione di raccomandazioni, o reiterati tentativi di ostacolare le segnalazioni), riferisce senza indugio tali fatti all'Amministratore Unico, per gli opportuni interventi. Inoltre, se emergono dalle segnalazioni elementi configurabili come reati o illeciti gravi, l'OdV coopera affinché l'ente proceda alle dovute comunicazioni alle Autorità competenti, in conformità ai requisiti normativi e a tutela dell'ente stesso.

In sintesi, il flusso informativo delineato garantisce che l'OdV sia costantemente informato e in grado di esercitare il proprio ruolo di vigilanza sul sistema di whistleblowing. Ciò è in linea con le migliori prassi e con le indicazioni fornite dalle Linee Guida ANAC e dalle prassi di Confindustria, le quali sottolineano la necessità di un coordinamento efficace tra il gestore del canale interno e gli organi di controllo interno, nonché di un'adeguata reportistica verso l'organo dirigente. L'OdV rappresenta il garante ultimo che le regole sancite in questa Parte Speciale siano effettivamente applicate e che il

sistema di gestione delle segnalazioni contribuisca concretamente alla prevenzione dei reati e alla diffusione di una cultura aziendale improntata alla legalità e alla trasparenza.

Destinatari della Parte Speciale: Si ribadisce che le disposizioni del presente documento si applicano a tutti i Destinatari del Modello 231 della Società, e dunque: ai componenti degli Organi Sociali, a tutti i dipendenti, nonché ai collaboratori esterni, consulenti e partner commerciali, nei limiti in cui essi interagiscano con la Società in relazione ai processi individuati come sensibili. Tutti i Destinatari sono tenuti a conoscere e rispettare le procedure di whistleblowing e le misure di tutela del segnalante, e a collaborare attivamente affinché il sistema funzioni in modo efficace. L'inosservanza di tali disposizioni, oltre a potenziali profili di responsabilità disciplinare e contrattuale, può pregiudicare il buon esito delle attività di prevenzione e rilevazione degli illeciti, mettendo a repentaglio l'esimente di responsabilità amministrativa dell'ente ai sensi del D.Lgs. 231/2001.

Protocolli specifici di prevenzione e informative all'OdV

Oltre a quanto espressamente previsto dai precedenti protocolli con riferimento a specifiche Attività Sensibili, i Referenti di P&P Technology srl trasmettono all'OdV le ulteriori informazioni individuate nelle procedure o negli altri Strumenti di attuazione del Modello applicabili, con la periodicità e le modalità previste dagli stessi.