


# PANTEX S.p.A.

Via Monte Grappa, 11 - 13888 MONGRANDO (BI)
Capitale sociale € 5.000.000,00 interamente versato
Cod. fisc. - P.I.V.A. - Reg. Imprese n. 00191480029
CCIAA Monte Rosa Laghi Alto Piemonte REA n. 103796

# Modello di organizzazione, gestione e controllo ex Decreto Legislativo 8 giugno 2001 n. 231



Indice

1. La Società e il settore di attività
2. Destinatari del Modello e definizioni
3. Quadro normativo di riferimento e aggiornamenti 2025
4. Finalità, principi e struttura del Modello
5. Il Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR)
6. Codice Etico ed Apparato sanzionatorio (Parte integrante del Modello)
7. Formazione, comunicazione e diffusione del Modello
8. Whistleblowing e flussi informativi verso l'OdV
9. L'Organismo di Vigilanza (istituzione, requisiti, budget e Regolamento)
10. Il Sistema Disciplinare e sanzionatorio
11. Parti Speciali (Protocolli di prevenzione reato per area/processo)
12. Gestione degli aggiornamenti del Modello
13. Allegati (matrici rischi/controlli, modulistica e clausole 231)
14. Reati presupposto



**1. La Società e il settore di attività**

La Pantex S.p.A. ha sede in Mongrando, in provincia di Biella, nel Piemonte settentrionale.

Ha un capitale di euro 5.000.000,00 interamente versato ed è iscritta al Registro delle Imprese tenuto dalla Camera di Commercio (CCIAA) Monte Rosa Laghi Alto Piemonte al numero 00191480029, che è anche il codice fiscale e la partita Iva della società).

La società, il cui nome deriva dal greco "pan" - tutto e "tex" - tessile, è nata a Biella nel 1972 per la nobilitazione e la commercializzazione delle materie prime per l'industria tessile laniera. È sorta dall'unione di differenti esperienze risalenti ai primi del 1900 maturate nei settori del lavaggio, del carbonizzo, della pettinatura e del recupero, selezione, garnettatura e riutilizzo dei sottoprodotti tessili di pettinatura, filatura e tessitura della lana.

Nel 1983 si è trasferita negli stabilimenti di Mongrando, sempre in provincia di Biella, dove sono state raggruppate le attività di battitura, sfioccatura miscelatura, tagliatura e cernita.

Dal 1985 a fianco dei sottoprodotti ha sviluppato una produzione di tops, open tops, lane lavate e carbonizzate, su tutta la gamma di finezze fornendo un importante servizio di stock service alla clientela italiana ed europea.

Dal 1977 e' membro attivo dell'Associazione Nazionale del Commercio Laniero.



Dispone di numerose certificazioni, tra cui:

Interwoollabs, Ethic.et, Responsible Wool Standard, Global Recycled Standard, Sustaina Wool Integrity Scheme, ISO 9001:2015, Global Organic Textile Standard.

La società pone la massima attenzione al benessere animale nell'approvvigionamento delle fibre di origine animale, agli aspetti ambientali e sociali.

Dove possibile vengono utilizzate lane certificate con standard internazionali riconosciuti e si evita l'utilizzo di fibre animali provenienti da specie in via di estinzione.

Nella trasformazione delle lane, si pone la massima attenzione a scegliere impianti in cui sono minimizzati i consumi di risorse energetiche e naturali, le emissioni inquinanti e dove possibile vengono riutilizzate le acque di processo, e' minimizzato l'utilizzo di sostanze chimiche nocive cosi' come il rischio per l'ambiente e per i lavoratori, viene privilegiato dove e' possibile l'acquisto di energia prodotta da fonti di energia rinnovabile, e' ridotta la produzione di rifiuti, avviene il recupero degli scarti di lavorazione non più utilizzabili come materie prime tessili, degli imballaggi e di tutto quello che può essere riciclato, sono rispettati i diritti fondamentali dei lavoratori e gli stessi non sono esposti a situazione che possano comportare rischi per loro salute e sicurezza.

Il lavoro di ciascuno è una risorsa molto importante che la società riconosce, valorizza e remunera correttamente.



L'azienda sociale acquista energia prodotta solo da fonti rinnovabili.

I criteri cui si ispira il presente documento sono quelli di legalità (tutti i destinatari del presente documento sono tenuti al rispetto della normativa vigente e delle norme interne aziendali), lealtà (tutte le attività, interne ed esterne, devono essere improntate alla massima lealtà ed integrità, operando con senso di responsabilità, in buona fede, stabilendo rapporti corretti e di collaborazione reciproca, nonché tendendo alla valorizzazione e salvaguardia del patrimonio dell'ente), trasparenza (tutte le azioni e le relazioni devono essere effettuate garantendo correttezza, completezza, accuratezza, uniformità e tempestività dell'informazione), imparzialità (l'ente, nelle relazioni sia interne che esterne, evita qualsiasi forma di discriminazione basata su età, sesso, orientamento sessuale, stato di salute, razza, nazionalità, opinioni politiche e sindacali e credenze religiose), diligenza e professionalità (Amministratori e Dipendenti svolgono diligentemente le proprie prestazioni professionali, operando nell'interesse dell'ente e perseguendo obiettivi di efficacia ed efficienza), riservatezza (nell'ambito dello svolgimento della propria attività, l'ente assicura la riservatezza dei dati personali e delle informazioni riservate di cui viene in possesso, le informazioni acquisite dai dipendenti e collaboratori appartengono all'ente medesimo e non possono essere utilizzate, comunicate o divulgate senza specifica autorizzazione) tutela dell'ambiente, della sicurezza e sviluppo sostenibile (l'ambiente é un bene primario che l'ente si impegna a salvaguardare. Le attività sono gestite nel rispetto della normativa vigente in materia di prevenzione e protezione e di tutela dell'ambiente. I dipendenti, nell'ambito delle proprie mansioni, partecipano al processo di prevenzione dei rischi, di salvaguardia dell'ambiente e di tutela della salute e della sicurezza nei confronti di se stessi, dei colleghi e di terzi)



L'organigramma completo è allegato e tenuto aggiornato.

**2. Destinatari del Modello e definizioni**

**Destinatari**: amministratori, sindaci/odv, dirigenti, dipendenti, collaboratori, agenti, consulenti, fornitori strategici, partner, appaltatori e subappaltatori nell'ambito delle **attività sensibili**.

**Attività Sensibili**: processi/operazioni nei quali può configurarsi una delle fattispecie di reato presupposto 231.

**Protocolli**: procedure, controlli e regole comportamentali adottate per presidiare i rischi-reato.



## 3. Quadro normativo e aggiornamenti 2025 (sintesi)

Il Modello recepisce:

D.Lgs. 231/2001 e successive integrazioni (catalogo reati presupposto, misure e sanzioni).

**Whistleblowing** D.Lgs. 24/2023: canali interni scritti/orali, tutela del segnalante, tempi, riservatezza, esternalizzazione canali e **ruolo OdV**.

**Reati tributari** (Parte speciale dedicata).

**Contrabbando / nuovo Codice doganale nazionale** (D.Lgs. 141/2024): profili rilevanti per import/export lane e fibre.

**Reati ambientali** (acque reflue, rifiuti, emissioni, ecoreati nel c.p.), **sicurezza sul lavoro** (D.Lgs. 81/2008), **reati informatici e strumenti di pagamento non-cash**, **delitti contro l'industria e il commercio**, **reati societari e contro la P.A.**

Linee guida di categoria e best practice di controllo interno.

## 4. Finalità, principi e struttura del Modello

**Finalità**: prevenire la commissione di reati nel corso delle attività aziendali; diffondere cultura della legalità; tutelare la Società da sanzioni 231; assicurare tracciabilità, trasparenza e segregazione dei compiti; delineare ruoli e responsabilità; disciplinare **flussi informativi** e **reporting** verso l'OdV.

**Principi cardine**: legalità, integrità, trasparenza, tracciabilità, proporzionalità dei controlli, accountability, miglioramento continuo, **tolleranza zero** verso corruzione, frodi, infortuni e illeciti ambientali.

**Struttura**: Parte Generale (Sez. 1-10), Parti Speciali per famiglie di reati (Sez. 11), Allegati operativi.



## 5. Sistema di Controllo Interno e Gestione dei Rischi

**Architettura**: CdA/AD; Funzioni di controllo; OdV (vigilanza su efficacia/attuazione Modello).

**Principi di controllo**: segregazione ruoli, doppio check/acquisti/pagamenti, poteri coerenti/deleghe, registrazioni tempestive/verificabili, conservazione documentale, tracciabilità fisica/contabile delle merci (balle/lotti), riconciliazioni, controllo accessi IT, logging e cybersecurity, controlli ambientali.

**Strumenti**: procedure operative/protocolli, files (gifts, conflitti d'interesse, controlli qualità), audit plan OdV.



**6. Codice Etico (parte integrante) – Apparato sanzionatorio (allegato)**

6.1 Introduzione

Il Codice richiama: normativa 231, linee guida di categoria, D.Lgs. 81/2008, D.Lgs. 152/2006, normativa doganale e fiscale, tutela dati personali, principi di sostenibilità e responsabilità sociale nella filiera tessile.

6.2 Destinatari, informazione e formazione

Il Codice è diffuso a tutti i Destinatari; è previsto **e-learning** e **formazione in aula** con test di apprendimento, onboarding per neoassunti e sessioni dedicate per apicali/aree a rischio.

6.3 Principi etici di riferimento

Integrità, legalità, concorrenza leale, trasparenza informativa, tracciabilità, tutela della salute e sicurezza, tutela ambiente e animali, rispetto dei diritti umani e **divieto di lavoro forzato/minorile** nella filiera, protezione di informazioni e dati, corretto uso di asset aziendali.

6.4 Norme di comportamento (sintesi)

**Rapporti con P.A.**: vietata qualsiasi forma di corruzione/induzione; gestione autorizzazioni ambientali/sicurezza e contributi pubblici con canali e ruoli formalizzati; rappresentanza verso enti pubblici solo da soggetti delegati.

**Gifts/Omaggi/Ospitalità**: consentiti solo se di **modico valore**, occasionali, leciti, tracciati nel **Files Omaggi** e approvati secondo procedura; mai per influenzare decisioni.

**Conflitti d'interesse**: obbligo di disclosure e astensione; registro conflitti.

**Acquisti e fornitori**: qualifica preventiva (due diligence 231, **sanzioni/embargo**, reputazione, aspetti etici/ambientali/REACH, antiriciclaggio in coerenza con 25-octies); contratti con **clausole 231** e diritto di audit.

**Dogane e commercio internazionale**: veridicità di origine, classificazione e valore; rispetto regimi preferenziali; divieto di triangolazioni fittizie.

**Gestione sostanze chimiche**: accettazione solo con **SDS REACH** valida e approvazione QAS; divieto di sostanze vietate (azoici vietati, PFC non conformi, ecc.).

**Ambiente**: rispetto titoli abilitativi (AUA/AIA); gestione rifiuti/ scarichi/emissioni; prevenzione sversamenti; piani di emergenza.

**Salute e sicurezza**: priorità alla prevenzione; DPI, formazione, manutenzioni, lock-out/tag-out; gestione appaltatori; near-miss reporting.

**IT e pagamenti**: protezione credenziali; uso carte/IBAN solo su anagrafiche qualificate e 4-eyes; divieto di cash improprio; presidi su strumenti di pagamento non cash.





**Comunicazione e marketing**: veridicità claim ambientali/sostenibilità; divieto greenwashing; tutela IP marchi e tracciabilità materiali riciclati/animali (es. RWS/RAS).
**Privacy e informazioni riservate**: trattamento lecito e minimizzazione; NDA dove necessario.
**Cooperazione con OdV**: dovere di informare e di collaborazione attiva.

## 7. Formazione, comunicazione e diffusione del Modello

**Piano formativo** con aggiornamento periodico:
**Base** (tutti): principi 231, Codice Etico, whistleblowing, nozioni di safety/ambiente/IT.
**Ruolo-specifica** (apicali, buyer, AFC, logistica/dogane, QAS, manutenzione, capi reparto, HR).
**Parte speciale**: moduli verticali su reati ambientali, sicurezza lavoro, tributari, PA/corruzione, contrabbando, strumenti di pagamento, informatici.
Tracciamento presenze e **test**; KPI: % formati, score medio test, azioni correttive.
**Comunicazione**: pubblicazione su intranet/sito; consegna a terzi delle **Linee di Condotta 231** e **clausole contrattuali**; campagne periodiche (poster, bacheche, micro-learning, phishing drill IT).

## 8. Whistleblowing e flussi informativi



8.1 Canali interni
**Piattaforma dedicata** (scritta/orale) con gestione sicura e separata;
**E-mail dedicata**: **odv@[dominio].it**;
**gestore esterno** per ricezione/triage.
**Tutele**: riservatezza/anonimato; divieto ritorsioni; protezione del segnalato in buona fede; informativa privacy; tempi di **ack** (7 gg) e riscontro (3 mesi, prorogabile).
**Ambito**: violazioni del Modello/Codice/legge; violazioni in materia di appalti, ambiente, sicurezza, dogane, tributario, frodi/riciclaggio, IT/security, diritti umani nella filiera.
**Registro segnalazioni** tenuto dall'OdV; conservazione **dati** secondo policy.

8.2 Flussi verso l'OdV (obbligatori)
Attivazioni/variazioni **AUA/AIA**, controlli ARPA/ATS/Ispettorato, verbali e prescrizioni;
**Infortuni** e near-miss, provvedimenti 81/08;
**Gestione rifiuti**: MUD, FIR, registri, anomalie;
**Dogane**: contestazioni/classificazioni, rettifiche, controlli scanner/canale rosso;
**Fiscale**: rilievi agenzia entrate/GdF, compensazioni, ruling;



**Tesoreria**: frodi pagamenti/IBAN, chargeback, anomalie carte;

**IT**: data breach, cyber-incidenti;

**HR**: procedimenti disciplinari 231-relevant;

**Aggiornamenti deleghe/procure**.

**9. Organismo di Vigilanza (OdV)**

9.1 Istituzione, composizione, requisiti

**Struttura**: OdV **monocratico** (con facoltà di migrare a collegiale in caso di crescita/complessità).

**Requisiti**: autonomia/indipendenza, professionalità, continuità di azione, onorabilità; assenza conflitti; accesso diretto al CdA.

**Nomina/Durata**: da CdA; durata 3 esercizi; rieleggibile; può dimettersi in qualsiasi tempo con effetto immediato; revoca solo per giusta causa.

**Budget**: **annuale dedicato** [€ 8.000,00] per consulenze, audit, formazione, piattaforme WB, spese legali/viaggio.

9.2 Poteri e funzioni



Accesso a dati/luoghi/documenti; richiesta informazioni a tutte le funzioni; avvalersi di ausiliari; ricezione/gestione WB; proposta misure correttive; reporting su rich. a CdA e Collegio Sindacale.

9.3 Regolamento OdV (sintesi)

Riunioni periodiche e/o ad hoc; verbali, annotazioni e/o **Action List**;

**Piano 231**: Dogane/Import, Pagamenti, Ambiente/Sicurezza, Acquisti/Agenti, Fiscale/IVA, IT Security;

**Reporting**: relazione al CdA;

**Gestione segnalazioni**: triage, istruttoria, esiti e raccomandazioni;

**Conservazione**: archivio digitale sicuro;

**Conflitti**: dovere di astensione e informativa;

**Riservatezza**: estesa anche post-mandato.

**10. Sistema Disciplinare (allegato)**

Destinatari e principio di proporzionalità

Si applica a dipendenti (nel rispetto altresì del **CCNL** applicato), dirigenti, apicali, componenti organi sociali, terzi (agenti/consulenti/appaltatori) tramite **clausole 231**. Sanzioni graduate per dolo/colpa,



gravità, reiterazione, ruolo, danno potenziale/effettivo, collaborazione.

**11. Parti Speciali – Protocolli di prevenzione per area/processo**

**Struttura**: per ciascuna famiglia di reati sono indicati **rischi tipici** del settore, **processi coinvolti**, **presidi organizzativi e controlli** (ex ante – in itinere – ex post), documenti e registri, ruoli RACI, indicatori di anomalia/red flags.

11.A Reati contro la P.A. (corruzione/induzione – contributi – frodi)

**Aree**: permessi e autorizzazioni (AUA/AIA, emissioni, scarichi, rifiuti), ispezioni, bandi/contributi pubblici, rapporti con dogane e agenzie fiscali.

**Presidi**: mappatura UO autorizzate al contatto con PA; registro incontri; regali/ospitalità tracciati; due firme su istanze e rendicontazioni; dossier probatori; **no cash**.

11.B Reati societari

**Aree**: bilancio e comunicazioni sociali; libri sociali; operazioni su capitale; rapporti con revisori.

**Presidi**: calendario di chiusura; check-list bilancio; reconciliazioni; verbali CdA/assemblea; segregazione redazione/controllo; **Policy Informativa Finanziaria**; archivio digitale a prova di manomissione.



11.C Ricettazione, riciclaggio e autoriciclaggio

**Aree**: incassi internazionali, trade finance, anticipi export, agenti esteri, vendite spot; approvvigionamenti da Paesi a rischio.

**Presidi**: **KYC terze parti** non periodiche (black list/sanzioni), coerenza economica operazione, tracciabilità fondi, canali bancari tracciati, verifica beneficiario effettivo, split duties tesoreria, alert su pagamenti atipici.

11.D Sicurezza sul lavoro (omicidio colposo/lesioni gravi – art. 25-septies)

**Aree**: reparti, movimentazione; agenti chimici/fisici/biologici, linee elettriche, appaltatori.

**Presidi**: DVR aggiornato e per rischi specifici; nomine e deleghe 81/08; formazione; **permessi di lavoro**; lock-out/tag-out; piani emergenza; verifica idoneità tecnico-professionale appaltatori; audit comportamentali; KPI infortuni/near-miss.




11.E Reati ambientali (art. 25-undecies)

**Aree**: gestione rifiuti/sottoprodotti, rumore.

**Presidi**: titoli AUA/AIA; piani di monitoraggio; bilanci di massa; registri rifiuti (FIR/RENTRI) e MUD; tracciabilità flussi; gestione fornitori rifiuti; verifiche laboratorio accreditato; gestione emergenze sversamenti; formazione addetti; audit ARPA readiness.

**Red flags**: superamenti limiti, smaltimenti anomali, cisterne senza registro, documenti incompleti, outsourcing non tracciato.

11.F Reati informatici e **strumenti di pagamento diversi dai contanti**

**Aree**: phishing su anagrafiche fornitori; frodi IBAN; carte aziendali; e-commerce B2B; sistemi IT/SCADA; dati clienti/fornitori.

**Presidi**: **change-control IBAN a doppia verifica**; limiti/spese carte; alert antifrode; firme digitali; MFA; backup; registro incident; segregazione reti OT/IT; log retention.

11.G Reati tributari

**Aree**: contabilizzazione, dichiarazioni, compensazioni, IVA intracomunitaria, TP, depositi doganali, regimi speciali.



**Presidi**: **Tax Control Framework** proporzionato; riconciliazioni; conservazione digitale fatture; controlli su compensazioni (monitoraggio F24); consulenza esterna su operazioni diverse; policy omaggi/costi deducibilità; monitoraggio scadenze.

11.H **Contrabbando** (nuovo codice doganale nazionale)

**Aree**: import extra-UE lane/fibre, classificazione doganale, origine e valore; regimi (perfezionamento, uso particolare), depositi doganali; accise ove rilevanti.

**Presidi**: **Dogana Compliance Program**: anagrafiche doganali, **classificazione tariffaria** con schede, dichiarazioni origine preferenziale/non preferenziale, **verifica valore** (incoterms/sconti), gestione rappresentanza doganale, **pre-clearing check-list**, audit spedizionieri.

11.I Delitti contro l'industria e il commercio / IP

**Aree**: qualità e conformità prodotti; dichiarazioni di composizione/origine; etichettatura; marchi; certificazioni tessili (GRS/RWS/ECOTEX).

**Presidi**: **Product Integrity Program**: laboratorio interno ed esterno; tracciabilità lotti; controlli etichette; tutela marchi/licenze; approvazione claim ambientali con evidenze; gestione reclami e richiami.



11.L Altre aree rilevanti (on top)

**Privacy e protezione dati** (coordinamento con consulente e sterno e con DPO);

**Responsabilità verso animali** (standard RWS/RAF): tracciabilità benessere animale).

**11.M – Aggiornamento normativo e presidi integrativi: intelligenza artificiale, misure restrittive dell'Unione europea, ambiente e filiera**

**11.M.1 – Finalità, ambito e coordinamento**

Il presente paragrafo integra il Modello di organizzazione, gestione e controllo di PANTEX S.p.A., aggiornando la valutazione dei rischi e i protocolli delle Parti Generale e Speciali alla normativa vigente al 9 ottobre 2026. Le prescrizioni si applicano ai Destinatari, secondo le rispettive funzioni, e ai terzi nei limiti degli obblighi contrattualmente assunti e delle disposizioni di legge.

L'aggiornamento considera sia l'introduzione o la modifica di reati presupposto sia i cambiamenti tecnologici, organizzativi e operativi capaci di incidere sulle modalità di commissione dei reati già contemplati. La responsabilità dell'ente resta subordinata ai presupposti stabiliti dal D.Lgs. 231/2001: non ogni inosservanza della normativa sull'intelligenza artificiale, della disciplina sulla protezione dei dati o degli standard di sostenibilità costituisce, per ciò solo, un illecito 231.

I controlli sono proporzionati alle attività effettivamente esercitate e alle risorse organizzative della Società. La ridotta consistenza dell'organico non giustifica l'assenza di controlli: quando non è concretamente possibile separare le funzioni, sono individuate verifiche compensative, documentate e svolte da un diverso amministratore o da un professionista incaricato. L'OdV conserva compiti di vigilanza e non assume la responsabilità della gestione operativa dei processi.



**11.M.2 – Intelligenza artificiale: quadro normativo e rilevanza 231**

Il Modello recepisce la legge 23 settembre 2025, n. 132, il D.Lgs. 9 settembre 2026, n. 160, e il regolamento (UE) 2024/1689, come modificato dal regolamento (UE) 2026/1744, nei rispettivi ambiti e secondo le relative disposizioni temporali. È incluso nella valutazione il nuovo art. 25-vicies del D.Lgs. 231/2001, introdotto dall'art. 15 del D.Lgs. 160/2026, con riferimento agli artt. 437-bis e 612-quater c.p. [1–3]

Le diverse date di applicazione degli obblighi europei sono considerate separatamente dall'entrata in vigore delle disposizioni penali nazionali. In particolare, l'applicazione differita delle disposizioni del capo III, sezioni 1, 2 e 3 dell'AI Act, salvo le eccezioni previste, al 2 dicembre 2027 per i sistemi dell'allegato III e al 2 agosto 2028 per quelli dell'allegato I non è intesa come esenzione generale dai divieti, dagli obblighi già applicabili o dalle regole di sicurezza e prevenzione del presente Modello. [3]

L'intelligenza artificiale è inoltre considerata una possibile modalità di realizzazione o agevolazione di reati già presidiati: falsità documentali rilevanti, frodi, reati societari, tributari, doganali, informatici, in



materia di pagamenti, proprietà intellettuale e sicurezza del lavoro. La valutazione distingue i casi in cui la Società possa essere coinvolta nella commissione dell'illecito da quelli in cui sia esclusivamente vittima di un attacco o di una frode.

**11.M.3 – Ricognizione, autorizzazione e responsabilità nell'impiego dei sistemi**

Il Consiglio di Amministrazione individua un amministratore responsabile del coordinamento dei presidi sull'intelligenza artificiale, avvalendosi, ove necessario, del consulente informatico e delle altre competenze aziendali o esterne. Non è richiesta, per effetto del presente paragrafo, la costituzione di un nuovo ufficio.

È tenuto un elenco aggiornato dei sistemi utilizzati per finalità aziendali, inclusi gli assistenti generativi, le funzionalità incorporate nei gestionali e gli strumenti impiegati da consulenti per trattare dati o svolgere attività per conto della Società. Per ciascuno sono individuati almeno fornitore, finalità, processo interessato, categorie di dati, utilizzatori autorizzati, responsabile, principali rischi, misure di controllo e data di approvazione. È verificato il ruolo della Società quale utilizzatore professionale e l'eventuale assunzione di ulteriori ruoli regolamentati.

Nuovi impieghi, collegamenti agli archivi aziendali o modifiche sostanziali delle funzionalità sono sottoposti a valutazione preventiva e autorizzazione. È vietato utilizzare account personali o strumenti non autorizzati per trattare dati aziendali riservati. Qualora non risultino impieghi di intelligenza artificiale, l'esito della ricognizione è documentato e riesaminato prima dell'introduzione di nuovi strumenti.



**11.M.4 – Supervisione umana, impieghi sensibili e sicurezza**

L'impiego dell'intelligenza artificiale ha funzione di supporto e non modifica le deleghe, i poteri di firma o le responsabilità assegnate. Gli elaborati destinati a decisioni rilevanti, comunicazioni esterne o adempimenti sono verificati da una persona competente, autorizzata e identificabile; il controllo non può ridursi a una conferma automatica dell'esito prodotto dal sistema.

Prima di destinare un sistema alla selezione o valutazione del personale, alla gestione di macchinari o a funzioni incidenti sulla sicurezza, sono verificati la classificazione del rischio, le condizioni di utilizzo, le istruzioni del fornitore e gli obblighi effettivamente applicabili. L'eventuale qualificazione ad alto rischio non è presunta per il solo fatto che il programma impieghi intelligenza artificiale.

Con riguardo all'art. 437-bis c.p., sono considerate le condotte di omissione delle misure di sicurezza o sorveglianza e di alterazione dei sistemi contemplate dalla norma. Per l'utilizzatore professionale assume specifico rilievo l'omissione intenzionale della sorveglianza umana sui sistemi ad alto rischio dalla quale derivi il pericolo richiesto dalla disposizione. [1]

Per gli impieghi sensibili autorizzati sono individuati il soggetto incaricato della supervisione, i controlli sugli esiti, le condizioni di arresto o sospensione e le modalità di gestione delle anomalie. Sono vietati l'aggiramento delle protezioni, le modifiche non autorizzate e l'utilizzo di un sistema quando anomalie

note impediscano di governarne adeguatamente i rischi. Gli impieghi sul personale devono rispettare i divieti europei applicabili, la dignità e la non discriminazione dei lavoratori e gli obblighi di informazione, protezione dei dati e disciplina dei controlli a distanza. [2–3]

**11.M.5 – Veridicità dei documenti, contenuti sintetici e protezione delle informazioni**

È vietato utilizzare l'intelligenza artificiale per creare, alterare o occultare documenti destinati a rappresentare fatti non veri, operazioni inesistenti, controlli mai eseguiti o certificazioni non possedute. Tale divieto riguarda, in particolare, fatture, registrazioni contabili, dichiarazioni fiscali e doganali, documenti di origine delle fibre, certificati di analisi, composizione e sostenibilità, tracciabilità dei lotti e documentazione di sicurezza e ambientale.

L'output di un sistema non costituisce, di per sé, prova dell'esattezza dei dati né sostituisce i documenti originali. Chi utilizza un elaborato verifica le fonti, i dati numerici, la coerenza con le evidenze aziendali e l'esistenza dei titoli o delle certificazioni richiamati. Le comunicazioni su origine, contenuto riciclato, benessere animale e qualità dei prodotti sono approvate soltanto sulla base di evidenze verificabili.

È vietato produrre o diffondere contenuti sintetici per impersonare persone, simulare ordini o autorizzazioni, screditare terzi o ingannare interlocutori. Il presidio comprende la diffusione illecita di immagini, video o voci generati o alterati con intelligenza artificiale di cui all'art. 612-quater c.p.; la configurazione del reato richiede gli elementi previsti dalla disposizione e non coincide con qualsiasi impiego di contenuti sintetici. Gli obblighi di trasparenza sono applicati nei casi, con le modalità e secondo le eccezioni dell'art. 50 dell'AI Act. [1–3]



Richieste di pagamento, modifiche di coordinate bancarie o istruzioni anomale non sono eseguite sulla sola base di messaggi, telefonate o videocomunicazioni apparentemente riconducibili a un soggetto autorizzato. Le verifiche aggiuntive sono effettuate tramite recapiti già conosciuti e indipendenti dal messaggio sospetto, conservandone evidenza.

È vietato immettere dati personali, segreti commerciali o documentazione riservata in servizi esterni senza preventiva valutazione e autorizzazione. Sono considerate le condizioni contrattuali, gli accessi, la conservazione, l'eventuale impiego dei dati per addestramento e i trasferimenti di dati. La registrazione delle attività è commisurata ai rischi e ai tempi legittimi di conservazione; non comporta la raccolta indiscriminata di ogni conversazione né l'introduzione di controlli illeciti sui lavoratori. Restano fermi i diritti di terzi su software, opere e banche dati.

**11.M.6 – Informazione e formazione**

Il piano di cui al paragrafo 7 comprende misure di alfabetizzazione sull'intelligenza artificiale proporzionate agli strumenti utilizzati, alle mansioni e alle competenze dei Destinatari, in coerenza con l'art. 4 dell'AI Act nel testo vigente. I contenuti riguardano limiti e possibili errori dei sistemi, tutela dei dati, verifica delle fonti, supervisione umana, frodi mediante contenuti sintetici, usi vietati e modalità di

comunicazione delle anomalie. [3]

La formazione, anche registrata, è accompagnata dalla documentazione della partecipazione e dalla verifica dell'apprendimento prevista dal Modello. Gli addetti alle attività sensibili ricevono istruzioni specifiche prima dell'impiego dei relativi strumenti. Gli aggiornamenti sono disposti quando cambiano sistemi, impieghi, rischi o prescrizioni rilevanti: nessun numero standard di ore né una scadenza biennale sono assunti come garanzia automatica di adeguatezza. La formazione sull'intelligenza artificiale non sostituisce quella obbligatoria in materia di salute e sicurezza.

**11.M.7 – Misure restrittive dell'Unione europea e commercio internazionale**

Il Modello recepisce il D.Lgs. 30 dicembre 2025, n. 211, con particolare riferimento all'art. 25-octies.2 del D.Lgs. 231/2001. I relativi presidi integrano le sezioni 11.C e 11.H e le regole di qualifica dei fornitori, gestione dei pagamenti e verifica delle operazioni con l'estero. [4]

La funzione commerciale e quella amministrativa, sotto la responsabilità dell'amministratore incaricato, verificano secondo criteri documentati l'identità delle controparti, gli assetti proprietari e di controllo rilevanti, i beneficiari dei pagamenti, le merci, i Paesi e le destinazioni coinvolti, nonché eventuali intermediari e percorsi anomali. Le verifiche sono effettuate prima dell'avvio del rapporto e dell'esecuzione delle operazioni esposte; sono aggiornate quando mutano le misure restrittive o gli elementi dell'operazione e con periodicità commisurata al rischio.



I controlli non si esauriscono nell'assenza del nominativo del contraente da una lista: sono considerate le ipotesi di disponibilità indiretta di fondi o risorse, le restrizioni merceologiche e i possibili meccanismi di elusione. Il ricorso a banche, spedizionieri o agenti non sostituisce le verifiche spettanti alla Società.

In presenza di una corrispondenza sospetta o di elementi incompatibili con le restrizioni applicabili, l'operazione è sospesa e sottoposta a verifica dell'amministratore competente, con supporto specialistico ove necessario. Sono documentati l'esito, le eventuali autorizzazioni e le condizioni da rispettare. Nessuna esigenza commerciale autorizza a frazionare o triangolare artificiosamente operazioni, falsificare l'origine o occultare il destinatario effettivo.

**11.M.8 – Ambiente, rifiuti, sottoprodotti e conformità dei materiali**

La sezione 11.E è integrata alla luce del D.L. 8 agosto 2025, n. 116, convertito dalla legge 3 ottobre 2025, n. 147, e del D.Lgs. 21 aprile 2026, n. 81. La valutazione considera l'art. 25-undecies nel testo vigente, comprese le nuove fattispecie e l'art. 452-bis.1 c.p. sul commercio di prodotti inquinanti, nei limiti dei relativi presupposti e dell'attività concretamente esercitata. [5]

Per le fibre, gli scarti tessili e gli altri materiali movimentati sono verificate e documentate, quando rilevanti, la qualificazione come prodotto, sottoprodotto o rifiuto, le condizioni del recupero, la destinazione e la corrispondenza fra documenti e movimentazioni effettive. L'attribuzione di una denominazione commerciale non sostituisce la verifica della corretta qualificazione giuridica del materiale.



I responsabili individuati nell'organigramma e nelle procedure verificano autorizzazioni, iscrizioni e requisiti degli operatori cui sono affidati trasporto, recupero o smaltimento; curano registrazioni e tracciabilità, inclusi gli adempimenti RENTRI ove applicabili. Per sostanze, impianti, scarichi ed emissioni effettivamente presenti sono riesaminati i rispettivi obblighi. Anomalie, documenti incoerenti o conferimenti privi di adeguato riscontro sono segnalati e non possono essere superati con sole dichiarazioni informali del fornitore.

**11.M.9 – Tutela delle persone e controlli sulla filiera**

Il Modello recepisce le modifiche del D.Lgs. 12 giugno 2026, n. 115, relative alla tratta e allo sfruttamento, compreso l'inserimento nell'art. 25-quinquies del reato di cui all'art. 601.1 c.p., concernente lo sfruttamento delle prestazioni di chi si sa essere vittima di riduzione in schiavitù o di tratta. [6]

La qualifica e il monitoraggio di fornitori, terzisti, appaltatori e operatori logistici considerano, secondo il rischio, regolarità del lavoro, ricorso a subaffidamenti, condizioni di impiego e attendibilità delle informazioni ricevute. Prezzi incompatibili con costi minimi plausibili, opacità nell'utilizzo della manodopera, limitazioni della libertà personale o segnalazioni credibili di sfruttamento richiedono approfondimenti e decisioni documentate.

Il Supplier Code of Conduct è coordinato con tali verifiche e con rimedi contrattuali concretamente utilizzabili. Il rapporto con un fornitore non determina automaticamente responsabilità per ogni illecito da questo commesso, ma non legittima a ignorare segnali attendibili di sfruttamento o a beneficiare consapevolmente di prestazioni illecite.



**11.M.10 – Flussi informativi, segnalazioni e sistema disciplinare**

I responsabili dei processi trasmettono all'OdV, almeno annualmente e in occasione di cambiamenti rilevanti, la ricognizione dei sistemi di intelligenza artificiale, le variazioni delle valutazioni di rischio, le iniziative formative e lo stato dei controlli integrativi. Sono comunicati senza ritardo incidenti significativi, impieghi non autorizzati, omissioni di supervisione, falsificazioni, anomalie relative a restrizioni internazionali, fatti ambientali rilevanti e segnalazioni attendibili di sfruttamento, con indicazione delle misure adottate.

I flussi ordinari verso l'OdV sono distinti dalle segnalazioni protette, che seguono la procedura whistleblowing e i canali effettivamente attivati ai sensi del D.Lgs. 24/2023. Il gestore delle segnalazioni è identificato con apposito atto; la coincidenza con l'OdV non è presunta. Identità, contenuti e documenti sono trattati con accessi limitati e nel rispetto delle tutele e dei termini di legge.

Le violazioni delle prescrizioni del presente paragrafo rilevano ai fini del sistema disciplinare del Modello, nel rispetto della legge, del CCNL e delle garanzie procedurali applicabili; per i terzi si applicano i rimedi previsti nei contratti. È vietato utilizzare sistemi automatizzati per individuare abusivamente i segnalanti, attuare ritorsioni o adottare sanzioni senza un'effettiva valutazione umana e il rispetto delle procedure.



### 11.M.11 – Attuazione, verifiche e aggiornamento documentale

Contestualmente all'approvazione dell'integrazione, il Consiglio di Amministrazione assegna responsabilità, risorse e tempi delle attività di attuazione e dispone l'aggiornamento della matrice rischi-controlli, dei flussi informativi, del piano formativo, delle clausole pertinenti e del catalogo dei reati presupposto. Le eventuali attività non ancora completate sono indicate come tali, con le misure transitorie di contenimento del rischio; il piano non differisce obblighi di legge già applicabili.

Per ogni rischio significativo la documentazione individua lo scenario, il controllo, chi lo esegue, quando lo esegue e l'evidenza da conservare. Il registro dei sistemi, le verifiche e le azioni correttive possono essere raccolti in un unico fascicolo o archivio aziendale, purché aggiornato, accessibile ai soggetti autorizzati e verificabile dall'OdV.

La revisione è attivata in occasione di novità normative rilevanti, nuovi processi o mercati, modifiche nell'impiego delle tecnologie, incidenti, significative violazioni o carenze dei controlli. Resta ferma la verifica annuale prevista dal paragrafo 12. L'OdV vigila sull'attuazione e propone correttivi; le decisioni organizzative e l'approvazione delle modifiche competono al Consiglio di Amministrazione.

L'inserimento del presente paragrafo non attesta che i presidi descritti siano già operativi né sostituisce la verifica della loro concreta attuazione. La versione approvata è identificata e annotata nel Registro revisioni con la data effettiva della deliberazione e con gli estremi degli allegati aggiornati.



## 12. Gestione delle revisioni del Modello

Il Modello è **vivo**: l'OdV propone aggiornamenti a seguito di novità normative/organizzative/eventi e verifica annualmente l'adeguatezza. Ogni revisione è approvata dal CdA.

## 13. Allegati operativi

Organigramma e sistema deleghe/procure

Matrice rischi e procedure sicurezza

Registro revisioni Modello

Piano Formazione periodico

Procedura Whistleblowing

Policy Dogane & Origine/Valore

Tax Control Framework

Clausole e moduli 231 per fornitori/consulenti/agenti/appaltatori



## 14. Reati presupposto

## 14. Reati presupposto — aggiornamento al 9 ottobre 2026

14.1. Famiglie previste dagli articoli 24 e seguenti del D.Lgs. 231/2001

Le denominazioni riportate nella tabella identificano le famiglie di reati, talvolta mediante una descrizione sintetica. Le singole fattispecie, i commi richiamati e le condizioni di responsabilità devono essere individuati nelle rispettive disposizioni.

| Riferimento | Famiglia di reati e principali precisazioni |
|---|---|
| Art. 24 | Erogazioni pubbliche, frodi a danno di soggetti pubblici e regolarità degli affidamenti. Comprende malversazione, indebite percezioni, truffe, frodi informatiche, frodi nelle pubbliche forniture e turbative delle procedure di affidamento, nei casi richiamati. |
| Art. 24-bis | Delitti informatici e trattamento illecito di dati. Comprende anche l'estorsione informatica dell'art. 629, terzo comma, c.p. |
| Art. 24-ter | Delitti di criminalità organizzata. |
| Art. 25 | Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione. Comprende anche il traffico di influenze illecite, secondo i richiami della disposizione. |
| Art. 25-bis | Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento. Include i richiami agli artt. 473 e 474 c.p. sulla contraffazione e sul commercio di prodotti con segni falsi. |
| Art. 25-bis.1 | Delitti contro l'industria e il commercio. Da coordinare con la L. 75/2026, che ha aggiunto il richiamo all'art. 517-octies, quarto comma, c.p., relativo alle condotte alimentari organizzate ivi previste. |
| Art. 25-ter | Reati societari. Comprende, fra gli altri, false comunicazioni sociali, illeciti sul capitale, corruzione tra privati, ostacolo alla vigilanza e false od omesse dichiarazioni per il certificato preliminare nelle operazioni transfrontaliere. |
| Art. 25-quater | Delitti con finalità di terrorismo o di eversione dell'ordine democratico, secondo i richiami al codice penale, alle leggi speciali e alla Convenzione internazionale sul finanziamento del terrorismo. |
| Art. 25-quater.1 | Pratiche di mutilazione degli organi genitali femminili, di cui all'art. 583-bis c.p. |
| Art. 25-quinquies | Delitti contro la personalità individuale. Comprende schiavitù, tratta, sfruttamento lavorativo e specifiche fattispecie riguardanti minori. Il D.Lgs. 115/2026 ha aggiunto l'art. 601.1 c.p., relativo all'approfittamento della vittima di riduzione in schiavitù o di |





| Riferimento | Famiglia di reati e principali precisazioni |
|---|---|
| | tratta. |
| Art. 25-sexies | Abusi di mercato: reati degli artt. 184 e 185 del D.Lgs. 58/1998, riguardanti informazioni privilegiate e manipolazione del mercato. |
| Art. 25-septies | Omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro. |
| Art. 25-octies | Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio: artt. 648, 648-bis, 648-ter e 648-ter.1 c.p. |
| Art. 25-octies.1 | Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori. Sono compresi gli ulteriori delitti contemplati dal comma 2 della disposizione. . |
| Art. 25-octies.2 | Reati in materia di violazione di misure restrittive dell'Unione europea. Introdotto dal D.Lgs. 211/2025: richiama gli artt. 275-bis, 275-ter e 275-quater c.p., limitatamente ai commi indicati, e l'art. 12, comma 1-bis, del D.Lgs. 286/1998. Gazzetta Ufficiale |
| Art. 25-novies | Delitti in materia di violazione del diritto d'autore, secondo i richiami alla L. 633/1941 contenuti nella disposizione. |
| Art. 25-decies | Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, di cui all'art. 377-bis c.p. |
| Art. 25-undecies | Reati ambientali. Il catalogo va letto tenendo conto della L. 147/2025 e del D.Lgs. 81/2026: comprende anche il commercio di prodotti inquinanti dell'art. 452-bis.1 c.p., oltre alle fattispecie espressamente richiamate in materia di inquinamento, rifiuti, controlli, bonifiche e tutela ambientale. |
| Art. 25-duodecies | Impiego di cittadini di paesi terzi il cui soggiorno è irregolare, nelle condizioni previste; comprende anche le specifiche fattispecie di favoreggiamento dell'immigrazione e della permanenza irregolari richiamate dalla disposizione. |
| Art. 25-terdecies | Razzismo e xenofobia, nei limiti del rinvio alle fattispecie oggi ricondotte all'art. 604-bis, terzo comma, c.p. |
| Art. 25-quaterdecies | Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati: artt. 1 e 4 della L. 401/1989. |
| Art. 25-quinquiesdecies | Reati tributari. Occorre distinguere le fattispecie del comma 1 da quelle del comma 1-bis, per le quali operano le condizioni relative alle frodi IVA transfrontaliere, precisate |





| Riferimento | Famiglia di reati e principali precisazioni |
|---|---|
| | sotto. |
| Art. 25-sexiesdecies | Contrabbando. Comprende i reati richiamati dalle disposizioni nazionali complementari al codice doganale dell'Unione, D.Lgs. 141/2024, e dal testo unico delle accise, D.Lgs. 504/1995. |
| Art. 25-septiesdecies | Delitti contro il patrimonio culturale. Sono quelli specificamente richiamati dalla disposizione: non tutti, indistintamente, i reati contenuti nel relativo titolo del codice penale. |
| Art. 25-duodevicies | Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici: artt. 518-sexies e 518-terdecies c.p. |
| Art. 25-undevicies | Delitti contro gli animali. Introdotto dalla L. 82/2025: artt. 544-bis, 544-ter, 544-quater, 544-quinquies e 638 c.p., con le esclusioni espressamente richiamate. |
| Art. 25-vicies | Reati commessi con l'uso di sistemi di intelligenza artificiale. Introdotto dal D.Lgs. 160/2026: richiama gli artt. 437-bis e 612-quater c.p. Non costituisce un rinvio generale a ogni violazione dell'AI Act. |

14.2. Ulteriori disposizioni da includere nel quadro generale



Art. 23 del D.Lgs. 231/2001 — Inosservanza delle sanzioni interdittive. È una specifica ipotesi di ulteriore responsabilità dell'ente per la trasgressione degli obblighi o divieti inerenti a sanzioni o misure cautelari interdittive, alle condizioni stabilite dalla disposizione.

Artt. 3 e 10 della L. 146/2006 — Reati transnazionali. Riguardano le specifiche fattispecie associative, in materia di immigrazione e di intralcio alla giustizia richiamate dall'art. 10, quando ricorrono i requisiti di transnazionalità dell'art. 3. Non basta che un qualsiasi reato presenti un collegamento con l'estero.

Parlamento

Art. 12 della L. 9/2013 — Responsabilità degli enti operanti nella filiera degli oli vergini di oliva. È una disciplina settoriale relativa a determinate fattispecie contro la salute pubblica, la fede pubblica e il commercio. Va richiamata nel quadro generale, senza presumere che sia applicabile all'attività tessile di PANTEX. I rinvii devono essere coordinati con le successive modifiche e abrogazioni.

14.3. Responsabilità per illeciti amministrativi di mercato: da tenere distinta

L'art. 187-quinquies del D.Lgs. 58/1998 disciplina la responsabilità dell'ente per determinate violazioni amministrative della normativa sugli abusi di mercato. Il relativo quadro, coordinato anche con il D.Lgs. 128/2026, deve restare separato: non è un'ulteriore famiglia di reati presupposto e non coincide con l'art. 25-sexies. Resta inoltre ferma la disciplina dei delitti tentati dell'art. 26 del D.Lgs. 231/2001: il tentativo non costituisce una famiglia autonoma, ma rileva nei limiti previsti dalla legge.

