Circolare Informativa in sigla SG&II
Sicurezza Giuridica & Informatica Integrata
(revisione novembre 2026)

Aggiornamento normativo, Organizzativo e Operativo per Imprese, Organi di Controllo e Organismi di Vigilanza

Avvertenza. La presente circolare ha finalità informativa e organizzativa. Le misure indicate devono essere calibrate sulla concreta struttura, sul settore, sulle dimensioni e sui rischi dell'ente; incentivi, scadenze e adempimenti richiedono una verifica aggiornata al momento dell'applicazione. Il testo tiene conto della normativa e della prassi pubblicate entro il 11 novembre 2026.

Questa circolare La riguarda?

Non tutti gli obblighi valgono per tutti. Qui sotto abbiamo raccolto le situazioni più ricorrenti: se riconosce la Sua impresa in una di esse, troverà nella circolare i riferimenti utili e, soprattutto, una ragione concreta per fissare una verifica.

1) Ha più di cinquanta dipendenti oppure un fatturato o un bilancio sopra i dieci milioni e opera nell'energia, nei trasporti, nella sanità, nelle acque, nel digitale, nell'alimentare, nella manifattura o nella gestione dei rifiuti? È probabile che rientri tra i soggetti NIS2. Dovrà registrarsi sul portale ACN, nominare il referente per gli incidenti e adottare misure di sicurezza verificabili entro i termini di legge, con responsabilità che risalgono fino agli amministratori.

2) Fornisce beni o servizi a un'impresa che rientra nella NIS2? Anche se la normativa non La obbliga direttamente, il Suo cliente è tenuto a controllare la sicurezza della propria filiera: si vedrà chiedere clausole contrattuali, questionari e audit. Arrivarci preparato è una condizione per non perdere la commessa.

3) Utilizza software di intelligenza artificiale – anche solo acquistato da terzi – per selezionare il personale, valutare clienti, assegnare turni o automatizzare decisioni? L'AI Act Le impone obblighi di trasparenza e di sorveglianza umana, e il nuovo reato 231

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

sull'IA rende l'impresa responsabile se quei sistemi non sono presidiati. Il punto non è chi ha scritto il software, ma chi lo usa.

4) Pubblica o diffonde contenuti creati o modificati con l'intelligenza artificiale – immagini, video, voci – nella comunicazione o nel marketing? Deve dichiararli come tali e valutare il rischio del reato di diffusione illecita di contenuti falsificati, oggi rilevante anche ai fini della responsabilità dell'ente.

5) Ha già adottato un Modello 231, o sta pensando di farlo? Il modello va aggiornato: tra i reati presupposto sono entrati quelli commessi con sistemi di IA e, da tempo, i reati informatici. Un modello fermo a qualche anno fa non è più idoneo, e l'idoneità è proprio ciò che il giudice valuta.

6) Supera i parametri dimensionali previsti per la rendicontazione di sostenibilità, oppure è una PMI quotata? Qui occorre distinguere con attenzione, perché il perimetro è in transizione. In base alla disciplina italiana oggi vigente, il d.lgs. 125/2024, l'obbligo riguarda le grandi imprese che superano due dei tre parametri tra cinquanta milioni di fatturato, venticinque milioni di attivo e duecentocinquanta dipendenti, oltre alle PMI quotate. La direttiva europea di semplificazione del 2026, il c.d. Omnibus I, innalza però in modo deciso tale soglia: una volta recepita in Italia, l'obbligo resterà alle sole imprese che abbiano, congiuntamente, più di mille dipendenti e oltre quattrocentocinquanta milioni di fatturato. Fino al recepimento continuano ad applicarsi le soglie attuali; da quel momento una parte delle imprese oggi tenute alla rendicontazione ne uscirà. Verificare in quale dei due scenari ci si collochi, e con quale tempistica, è il primo passo, anche perché banche e grandi committenti continueranno a chiedere questi dati lungo la filiera. Un'avvertenza utile per chi oggi supera le soglie ma non raggiungerà quelle future: fino al recepimento l'obbligo resta e va assolto; per chi è destinato a uscire dal perimetro conviene nondimeno un adeguamento proporzionato, calibrato sulle informazioni che la filiera continuerà a richiedere anziché su una rendicontazione completa che potrebbe non divenire mai dovuta.

7) Ha in programma investimenti in tecnologia, sicurezza informatica o sistemi di IA nel 2026? L'iperammortamento che ha sostituito i precedenti crediti d'imposta può ridurre sensibilmente il costo, ma a condizioni precise: conta la natura del bene, l'interconnessione ai processi e una comunicazione da inviare prima dell'ordine. Muoversi dopo l'acquisto, spesso, significa perdere il beneficio.

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

Se anche uno solo di questi casi La riguarda, vale la pena di approfondire. La verifica preliminare serve proprio a questo: distinguere ciò che è davvero cogente per la Sua impresa da ciò che non lo è, evitando sia gli allarmismi sia le sorprese.

In sintesi

Tra la fine del 2025 e il 2026 molte delle regole che governano l'impresa digitale sono state riscritte, e quasi sempre con scadenze vicine. Abbiamo raccolto in questa circolare ciò che oggi conta davvero, mostrando come adempimenti nati in ambiti diversi – la responsabilità degli enti, la sicurezza informatica, l'intelligenza artificiale, i dati, la sostenibilità, il fisco – finiscano per intrecciarsi. È il senso del modello che adottiamo, SG&II, Sicurezza Giuridica & Informatica Integrata. Ecco, in breve, di cosa parliamo.

– Quando un Modello 231 regge davvero al vaglio del giudice, alla luce delle sentenze arrivate fino al 2026, e che ruolo ha l'Organismo di Vigilanza.

– L'intelligenza artificiale, che ora entra anche nel penale d'impresa: il nuovo art. 25-vicies del d.lgs. 231/2001, gli obblighi di trasparenza dell'AI Act e le scadenze ridisegnate dal Digital Omnibus.

– La NIS2 e la sicurezza informatica: chi deve adeguarsi, quali misure servono, come si notificano gli incidenti e perché la filiera è parte del problema.

– I dati e le persone: fin dove arrivano i controlli sul lavoro, come si gestiscono le segnalazioni e cosa chiede il GDPR.

– La sostenibilità (CSRD ed ESRS), con un calendario che le semplificazioni europee hanno appena cambiato e che pesa su banche e rapporti di fornitura.

– Gli incentivi fiscali del 2026: l'iperammortamento che ha preso il posto dei vecchi crediti d'imposta e a quali condizioni se ne può approfittare.

Nessuno di questi fronti vive da solo: tenere insieme governance, dati, sicurezza, persone e tecnologia è ciò che distingue un'impresa che previene da una che rincorre. Una verifica preliminare serve a capire quali di queste regole La riguardino davvero, e da dove conviene cominciare.

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

1. Premessa e finalità

La trasformazione digitale impone alle imprese di governare, con metodo e proporzionalità, rischi giuridici, tecnologici e reputazionali. Non è un approccio allarmistico: è una scelta (necessaria) di competitività, continuità operativa e tutela del patrimonio aziendale. Dati, *software*, processi automatizzati, *know-how* e relazioni di filiera sono oggi componenti essenziali del valore d'impresa.

SG&II – Sicurezza Giuridica & Informatica Integrata – è il modello di tutela legale a sistema integrato, preventivo, di monitoraggio e di pronto intervento adottato dallo Studio. Esso coordina le *policy* aziendali, *compliance* 231, codice antimafia, *privacy*/GDPR, *cybersecurity* e NIS2, AI *governance*, proprietà intellettuale e sostenibilità/CSRD (*Corporate Sustainability Reporting Directive*; Dir. (UE) 2022/2464).[1]

Il *leitmotiv* è quello delle tre P: **Prevedere, Prevenire, Prosperare**.

"Prevedere" rappresenta la capacità, organizzata, di identificare i segnali di rischio; "prevenire" significa adottare presidi efficaci e verificabili; "prosperare" vuol dire trasformare la conformità in affidabilità, efficienza e vantaggio competitivo.

[1]La Dir. (UE) 2022/2464 ha trasformato la rendicontazione di sostenibilità da adempimento volontario in obbligo di legge: le informazioni confluiscono nella relazione sulla gestione, con regole e controlli analoghi a quelli del bilancio d'esercizio. Gli standard applicabili sono gli ESRS – *European Sustainability Reporting Standards* – adottati con Reg. delegato (UE) 2023/2772: dodici standard, di cui due trasversali e obbligatori per tutti (ESRS 1 e ESRS 2) e dieci tematici, ripartiti nei tre pilastri ESG.
E – Environment (cinque standard): E1 Clima, con emissioni Scope 1, 2 e 3, E2 Inquinamento, E3 Acqua e risorse marine, E4 Biodiversità ed ecosistemi, E5 Uso delle risorse ed economia circolare.
S – Social (quattro standard): S1 Forza lavoro propria, cui si riconducono i profili rilevanti ai fini dell'art. 603-bis c.p., S2 Lavoratori nella catena del valore, S3 Comunità interessate, S4 Consumatori e utilizzatori finali.
G – Governance: un solo standard tematico, G1 Condotta delle imprese, che copre anticorruzione, *whistleblowing*, cultura d'impresa e rapporti con i fornitori. A questi dieci standard tematici si aggiungono i due trasversali, ESRS 1 e ESRS 2, obbligatori per tutti i soggetti rendicontanti.
La novità di maggiore impatto è la cosiddetta doppia materialità, che impone di rendicontare su due fronti:
1. Materialità d'impatto: come l'azienda impatta sul mondo (es. inquini, sfrutti?)
2. Materialità finanziaria: come il mondo impatta finanziariamente (es. il cambiamento climatico fa perdere o fallire?)
Se uno dei due è rilevante, si deve rendicontarlo.
La prima ondata, costituita dagli enti di interesse pubblico di grandi dimensioni con più di cinquecento dipendenti, rendiconta dall'esercizio 2024. Per le altre categorie il calendario è stato differito di due anni dalla Dir. (UE) 2025/794, recepita con la L. 8 agosto 2025, n. 118: le grandi imprese che superano due dei tre parametri dimensionali (fatturato netto 50 milioni di euro, totale attivo 25 milioni di euro, 250 dipendenti) rendicontano dall'esercizio 2027 e le PMI quotate dall'esercizio 2028. Il profilo di conformità rileva anche sul piano economico, poiché gli enti creditizi soggetti a rendicontazione propria e i clienti tenuti a rendicontare la catena del valore ai sensi dell'ESRS S2 trasferiscono a monte le proprie esigenze informative, con effetti sull'accesso al credito, sulla permanenza nei rapporti di fornitura e sulla valutazione dell'impresa nelle operazioni straordinarie. In conclusione, la CSRD colloca gli indicatori ESG nella relazione sulla gestione, soggetta ad attestazione di conformità da parte del revisore. **Il successivo Pacchetto Omnibus I, recepito nella Direttiva (UE) 2026/470, ha modificato in modo significativo il quadro della rendicontazione di sostenibilità, restringendo il perimetro soggettivo della CSRD e semplificando gli obblighi di reporting. La direttiva è entrata in vigore il 18 marzo 2026, ma deve essere recepita dagli Stati membri entro il 19 marzo 2027; pertanto, per la pianificazione aziendale occorre coordinare il nuovo quadro europeo con la disciplina nazionale vigente e con le relative misure di recepimento.**

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

2. Quadro normativo integrato

- d.lgs. 8 giugno 2001, n. 231: gli artt. 6 e 7 disciplinano l'esimente dell'ente, fondata su un modello idoneo ed efficacemente attuato, su un Organismo di Vigilanza autonomo e su un sistema di controllo coerente con i rischi concreti. Le Linee guida Confindustria e di categoria costituiscono un rilevante riferimento metodologico ai fini dell'art. 6, comma 3, del decreto.
- Salute e sicurezza: l'art. 30, d.lgs. 9 aprile 2008 n. 81disciplina i sistemi di gestione della salute e sicurezza sul lavoro; il comma 5 presume conformi i modelli definiti secondo le linee guida UNI-INAIL del 2001 o secondo il BS OHSAS 18001:2007; quest'ultimo *standard* è stato ritirato nel marzo 2021 ed è oggi sostituito dalla UNI ISO 45001:2018, unico riferimento certificabile.
- *Whistleblowing*: il d.lgs. 10 marzo 2023, n. 24, le Linee guida ANAC di cui alla Delibera n. 311 del 12 luglio 2023 e i successivi aggiornamenti richiedono canali interni riservati, avviso di ricevimento entro sette giorni dalla ricezione e riscontro entro tre mesi da tale avviso o, in mancanza, dalla scadenza dei sette giorni (art. 5 d.lgs. 24/2023), oltre alla protezione contro le ritorsioni. Nel settore privato l'obbligo di canale interno grava sugli enti che hanno impiegato nell'ultimo anno almeno cinquanta lavoratori subordinati e, a prescindere dal numero, sugli enti che adottano un modello ex d.lgs. 231/2001 e su quelli operanti nei settori indicati dall'art. 2, comma 1, lett. *q*), n. 3, del medesimo decreto.
- *Privacy*: il Reg. (UE) 2016/679 impone *accountability*, minimizzazione, sicurezza, trasparenza e gestione dei *data breach*; sono rilevanti le indicazioni EDPB su *dark patterns* e violazioni di dati, in particolare le Linee guida EDPB 3/2022 sui *dark patterns* e le Linee guida 9/2022 sulla notifica delle violazioni. Per il trattamento dei dati nelle segnalazioni interne si rinvia alle Linee guida ANAC approvate con delibera n. 311 del 12 luglio 2023, adottate previo parere del Garante.
- Cyber/NIS2: la Dir. (UE) 2022/2555 è stata recepita dal d.lgs. 4 settembre 2024, n. 138. Occorre considerare, tra l'altro, la determinazione ACN 19 dicembre 2025, n. 379907, applicabile dal 15 gennaio 2026, che ha sostituito la determinazione 14 aprile 2025, n. 164179, e il *Framework* Nazionale *Cybersecurity* & *Data Protection*, ed. 2025. I termini di adeguamento sono differenziati: per i soggetti iscritti nell'elenco NIS nel corso del 2025 le misure di sicurezza di base vanno adottate entro

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

diciotto mesi dalla comunicazione di inserimento; per quelli iscritti per la prima volta nel 2026 il termine scade il 31 luglio 2027. Gli obblighi di notifica degli incidenti significativi decorrono dal nono mese successivo alla medesima comunicazione.

- Sostenibilità: la Dir. (UE) 2022/2464 (CSRD), il Reg. delegato (UE) 2023/2772 sugli ESRS e il d.lgs. 125/2024 richiedono un sistema di rendicontazione e controlli interni fondato, tra l'altro, sugli ESRS 1, ESRS 2 e sugli standard tematici. Il calendario applicativo è stato differito di due anni per le imprese non appartenenti alla prima ondata dalla Dir. (UE) 2025/794, c.d. *"stop the clock"*: recepita in Italia con la L. 8 agosto 2025, n. 118, di conversione del D.L. 30 giugno 2025, n. 95. La successiva **2026/470**, di **semplificazione dell'Omnibus I**, entrata in vigore il **18 marzo 2026,** modifica direttamente la disciplina della CSRD e della CSDDD, oltre alle direttive contabili e di revisione. Il termine ordinario di recepimento delle modifiche CSRD è il **19 marzo 2027**. Sul piano soggettivo, la direttiva innalza in modo sensibile le soglie: una volta recepita, l'obbligo di rendicontazione resterà alle sole imprese che superino, congiuntamente, i mille dipendenti e i 450 milioni di euro di fatturato, con un perimetro quindi assai più ristretto rispetto a quello attuale. Fino al recepimento, tuttavia, continuano ad applicarsi le soglie dimensionali previste dalla disciplina nazionale vigente (d.lgs. 125/2024).
- Diritto d'autore: la L. 22 aprile 1941, n. 633 e l'art. 25-*novies* d.lgs. 231/2001 impongono presidi su software, licenze, contenuti, repository e utilizzi digitali; la L. 132/2025 è intervenuta anche sulla disciplina d'autore in relazione ai contenuti generati con sistemi di intelligenza artificiale.
- AI *governance*: il Reg. (UE) 2024/1689 (AI Act) adotta un approccio basato sul rischio. Per gli utilizzatori (*deployer*) assumono rilievo l'art. 26 e, dal 2 agosto 2026, gli obblighi di trasparenza dell'art. 50. Il Reg. (UE) 2026/1744 ("Digital Omnibus") ha modificato il calendario di applicazione dell'AI Act, differendo alcune disposizioni relative ai sistemi di AI ad alto rischio – al 2 dicembre 2027 per l'Allegato III e al 2 agosto 2028 per l'Allegato I. Restano distinti gli obblighi di alfabetizzazione e gli obblighi di trasparenza di cui all'art. 50, secondo le rispettive date di applicazione.

  In materia di AI, rileva, inoltre, il d.lgs. 9 settembre 2026, n. 160, pubblicato nella G.U. n. 214 del 15 settembre 2026 (in vigore dal 30 settembre 2026) che, all'art. 15, ha introdotto nel d.lgs. 231/2001 il nuovo **art. 25-*vicies***, **"*Reati commessi con l'uso***

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

***di sistemi di intelligenza artificiale*"**, includendo il reato c.d. di "*deepfake"*, di cui all'art. 612-*quater* c.p.**,** nel catalogo dei reati presupposto della responsabilità degli enti ai sensi del d.lgs. 231/2001. Il nuovo art. 25-*vicies* non si esaurisce peraltro nel *deepfake*: esso richiama altresì il nuovo art. 437-*bis* c.p., che punisce l'omessa adozione delle misure di sicurezza e di sorveglianza umana sui sistemi di intelligenza artificiale ad alto rischio e la loro alterazione illecita. È proprio quest'ultima fattispecie a rilevare in via diretta per l'impresa che utilizza sistemi di IA ad alto rischio, imponendo di presidiarne la sicurezza e il controllo umano a monte del rischio di diffusione di contenuti sintetici. La fattispecie di *deepfake*, introdotta dalla L. 23 settembre 2025, n. 132, punisce, con la reclusione da uno a cinque anni, chiunque cagioni un danno ingiusto a una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità. La rilevanza ai fini 231 impone, quindi, alle imprese di considerare anche il rischio connesso alla produzione e diffusione di contenuti sintetici nell'ambito dei propri presidi organizzativi e di controllo.

3. MOG 231: requisiti essenziali e giurisprudenza chiave

Un MOG idoneo non è un documento standardizzato: deve essere *tailor-made*, costruito sui processi, sui reati presupposto e sulle effettive modalità operative dell'ente. I requisiti essenziali comprendono: mappatura dei rischi-reato; protocolli decisionali e di controllo; codice etico; sistema disciplinare; formazione; canali di segnalazione; OdV autonomo, indipendente e dotato di adeguati poteri; flussi informativi e aggiornamento periodico. Molti sono, per altro, in filiera, i soggetti destinatari dei modelli e delle normative esaminate, indipendentemente dall'adozione di presidi ad opera dei committenti, ovvero che hanno facoltà di rifiutarsi di proseguire o avviare il rapporto e/o di segnalare le anomalie (dalla PA, ai privati: consulenti dell'impresa, fornitori, dipendenti. Il modello non esaurisce gli obblighi organizzativi dell'ente. Restano evidentemente distinti, con presupposti e destinatari propri, il dovere di istituire assetti adeguati alla rilevazione tempestiva della crisi (art. 2086, secondo comma, c.c. e art. 3 d.lgs. 14/2019), gli obblighi di segnalazione degli organi di controllo (art. 25-*octies*.1 CCII) e dei creditori pubblici

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

qualificati (art. 25-*novies* CCII) e gli obblighi antiriciclaggio gravanti sui soggetti indicati dall'art. 3 d.lgs. 231/2007.

Giurisprudenza e dottrina confermano che l'idoneità del modello deve essere valutata in concreto, secondo il criterio della prognosi postuma, verificando se il modello, quale concretamente adottato e attuato, fosse idoneo a prevenire reati della specie di quello verificatosi. L'efficacia del sistema dipende, pertanto, dalla sua effettiva attuazione, dall'operatività dei controlli e dei flussi informativi e dalla capacità dell'organizzazione di rilevare e reagire alle anomalie. In presenza di modelli conformi ai codici di comportamento elaborati ai sensi dell'art. 6, comma 3, d.lgs. 231/2001, il giudizio di inidoneità richiede una motivazione puntuale, fermo restando che la conformità alle linee guida costituisce un parametro di valutazione e non esclude la verifica dell'adeguatezza del modello rispetto alla concreta struttura dell'ente e agli specifici rischi-reato.

In questa prospettiva si colloca Cass. pen., Sez. VI, 15 giugno 2022, n. 23401 (Impregilo), che ha valorizzato il criterio della prognosi postuma, il ruolo delle linee guida e l'autonomia, i compiti e i poteri dell'Organismo di Vigilanza. L'indirizzo è stato ulteriormente sviluppato dalla giurisprudenza successiva, che riconduce la responsabilità dell'ente alla dimostrazione di una specifica "colpa di organizzazione", evitando che essa possa essere desunta automaticamente dalla mera verificazione del reato presupposto o dalla sola mancanza o inidoneità del modello. In particolare, più recentemente, Cass. pen., Sez. IV, 4 marzo 2026, n. 8397 ha ribadito che la mancanza, l'inidoneità o l'inefficace attuazione del modello non sono, di per sé, sufficienti a fondare la responsabilità dell'ente, essendo necessario accertare un concreto deficit organizzativo, consistente nell'omessa predisposizione di cautele organizzative e gestionali idonee a prevenire reati della specie di quello verificatosi.

In materia di salute e sicurezza sul lavoro, assume particolare rilievo anche il rapporto tra modello organizzativo e sistemi di gestione certificati. Cass. pen., Sez. IV, 15 maggio 2025, n. 18410 ha evidenziato che la conformità del sistema a standard riconosciuti non esaurisce la verifica giudiziale, che deve investire anche la concreta ed effettiva attuazione delle procedure. Cass. pen., Sez. IV, 1° settembre 2025, n. 30039 ha, per altro verso, precisato che il modello 231 non è chiamato a contenere prescrizioni tecnico-operative di dettaglio, proprie di altri strumenti aziendali, ma deve delineare principi, procedure generali, controlli e flussi informativi aventi carattere generale e sistematico; la conformità del sistema organizzativo a standard internazionali, pur non determinando automaticamente

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

l'esenzione da responsabilità, costituisce un elemento qualificato, il cui superamento richiede una puntuale dimostrazione della sostanziale inadeguatezza del sistema adottato.
Il quadro è stato nel frattempo rafforzato sul piano normativo dalla modifica dell'art. 30, comma 5, d.lgs. 81/2008, operata dal D.L. 159/2025, conv. dalla l. 29 dicembre 2025, n. 198, che ha sostituito il precedente riferimento allo standard OHSAS 18001:2007 con quello alla UNI EN ISO 45001:2023+A1:2024, prevedendo che i modelli definiti conformemente a tale norma si presumano conformi ai requisiti dell'art. 30 per le parti corrispondenti. Resta comunque necessaria, anche alla luce della giurisprudenza richiamata, la verifica dell'effettiva attuazione e operatività del sistema.
Quanto alle pronunce di più immediata attualità, la decisione Cass. pen., Sez. IV, 4 agosto 2026, n. 29592, relativa al disastro ferroviario di Viareggio, ha definito il nuovo giudizio di legittimità in relazione a profili ormai prevalentemente sanzionatori, nel quadro degli accertamenti di responsabilità progressivamente consolidatisi nei precedenti giudizi. Tale vicenda giudiziaria conferma la centralità, nelle organizzazioni complesse, del governo effettivo del rischio e dell'adeguatezza degli assetti organizzativi: la ripartizione interna di funzioni e responsabilità non esaurisce gli obblighi prevenzionistici quando l'evento trovi origine in carenze di carattere strutturale e organizzativo. La più recente Cass. pen., Sez. IV, 4 agosto 2026, n. 29592, chiude la complessa vicenda processuale di Viareggio su profili ormai prevalentemente sanzionatori, nel quadro degli accertamenti di responsabilità progressivamente consolidatisi nei precedenti giudizi.
Resta invece in attesa del deposito delle motivazioni la sentenza del Tribunale di Genova del 16 luglio 2026 relativa al crollo del viadotto Polcevera. Dal dispositivo risulta l'esclusione sia della c.d. aggravante lavoristica sia della circostanza della colpa cosciente di cui all'art. 61, n. 3, c.p. L'esclusione dell'aggravante connessa alla violazione delle norme per la prevenzione degli infortuni sul lavoro assume potenziale rilievo rispetto al perimetro applicativo dell'art. 25-septies d.lgs. 231/2001; la portata della decisione sotto tale profilo dovrà tuttavia essere valutata alla luce delle motivazioni, non essendo prudente desumere dal solo dispositivo conclusioni definitive sul relativo fondamento giuridico.

4. Integrazioni *cross-compliance* da inserire nel SG&II

La matrice integrata deve correlare le macro-aree 231 – artt. 24, 24-*bis*, 24-*ter*, 25, 25-*bis*, 25-*bis*.1, 25-*ter*, 25-*quinquies*, 25-*sexies*, 25-*septies*, 25-*octies*, 25-*octies*.1, 25-octies.2, 25-

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

novies, 25-*decies*, 25-*undecies*, 25-*duodecies*, 25-*terdecies*, 25-*quinquiesdecies* e 25-*sexiesdecies* – ai rischi del Codice antimafia (artt. 34 e 34-*bis* d.lgs. 159/2011, oltre agli artt. 67, 84, 91 e 94-*bis* in materia di documentazione antimafia e di misure amministrative di prevenzione collaborativa), GDPR, NIS2, CSRD/ESRS, IP e AI Act.

- PA e anticorruzione: due diligence su terzi, segregazione dei poteri, regole su omaggi e ospitalità, tracciabilità dei contatti con la PA.
- Reati informatici: *identity and access management*, *hardening*, *patching*, *logging*, *incident response*, controllo dei fornitori ICT e sicurezza della *supply chain* in coerenza con NIS2.
- Societari e mercati: controlli sul bilancio, operazioni con parti correlate, insider list, barriere informative e conservazione della documentazione.
- Salute, ambiente e HSE: SGSL, *audit*, manutenzioni, *near miss*, autorizzazioni AUA/AIA, rifiuti, emissioni, scarichi e piani di emergenza.
- Riciclaggio e rapporti finanziari: KYC, tracciabilità dei pagamenti, *red flag*, *escalation* e controlli sui terzi.
- Misure restrittive UE ed export control: screening delle controparti e dei beneficiari effettivi, verifica delle liste di sanzioni, controlli sulle operazioni di import/export, gestione delle autorizzazioni e dei divieti applicabili, tracciabilità delle verifiche e procedure di escalation per le anomalie, anche ai fini della valutazione del rischio ex art. 25-octies.2 d.lgs. 231/2001.
- Reati tributari: verifica dei fornitori e del ciclo passivo, controlli su inerenza ed effettività delle operazioni, tracciabilità della documentazione a supporto delle dichiarazioni, procedure di gestione dei crediti d'imposta e delle compensazioni (art. 25-*quinquiesdecies* d.lgs. 231/2001).
- Copyright, HR e DEI (*Diversity, Equity and Inclusion*): inventario degli asset, licenze *software*, *policy* sui *repository*, formazione antidiscriminazione, verifiche documentali e canali di segnalazione.
- Whistleblowing e GDPR: gestione riservata delle segnalazioni, segregazione degli accessi, DPIA ove necessario, *retention*, *data breach management* e *accountability*.

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

5. AI *governance* e funzioni di controllo

L'impresa deve censire tutti i sistemi di AI utilizzati, anche quelli forniti da soggetti esterni, e classificarli in base alla finalità e al livello di rischio. Per ciascun sistema devono essere definiti un responsabile (*owner*), regole di utilizzo e controlli adeguati.
Per i sistemi ad alto rischio sono richiesti presidi più rigorosi: gestione dei rischi, qualità e *governance* dei dati, verifica di eventuali *bias*, tracciabilità, registrazione delle attività, supervisione umana, *cybersecurity* e trasparenza verso gli utenti.
Queste misure devono essere integrate con gli altri processi aziendali di *compliance*, in particolare con la DPIA prevista dalla normativa *privacy* e con la gestione degli incidenti prevista dalla NIS2.
Il differimento del regime dell'alto rischio non sospende l'obbligo di alfabetizzazione in materia di AI di cui all'art. 4 dell'AI Act, applicabile dal 2 febbraio 2025.
I Report periodici (flussi informativi) verso l'OdV devono riguardare i sistemi utilizzati, modifiche rilevanti, incidenti, non conformità, risultati degli audit, reclami, segnalazioni *whistleblowing* e *remediation*. L'OdV verifica l'effettività dei presidi, senza sostituirsi alla gestione operativa.

6. *Privacy*, controlli difensivi e CEDU/CGUE

I controlli nei luoghi di lavoro richiedono una valutazione di necessità, proporzionalità, trasparenza e minimizzazione. I principi espressi dalla Corte EDU in Bărbulescu c. Romania (Grande Camera, 5 settembre 2017) e López Ribalda c. Spagna (Grande Camera, 17 ottobre 2019) incidono sulla delimitazione dei controlli e sul bilanciamento tra esigenze difensive, dignità e riservatezza del lavoratore. In ambito nazionale il perimetro resta segnato dall'art. 4 L. 300/1970, come modificato dall'art. 23 d.lgs. 151/2015, e dalla categoria dei controlli difensivi in senso stretto, ammessi soltanto a fronte di un fondato sospetto già insorto. In tal senso, Cass. civ., Sez. lav., 26 giugno 2023, n. 18168, Rv. 668092-01, che distingue i controlli difensivi in senso stretto da quelli a tutela del patrimonio aziendale, gravando sul datore di lavoro l'onere di allegare e provare le specifiche circostanze che hanno determinato l'attivazione del controllo tecnologico ex post, indicando elementi indiziari, materiali e riconoscibili, non espressione di un mero convincimento soggettivo, idonei a concretare il fondato sospetto della commissione di comportamenti illeciti. La Suprema Corte ha, inoltre, affermato il seguente principio di

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

diritto in materia di protezione dei dati personali: «*Il rilievo che, per i controlli difensivi in senso stretto, non opera la disciplina speciale dettata dall'art. 4 dello Statuto dei Lavoratori, come novellato, non esclude il rispetto della disciplina generale prevista per la protezione dei dati personali, di cui al d.lgs. n. 196 del 2003 e al Regolamento UE 2016/679 (GDPR), con particolare riferimento agli incombenti informativi di cui all'art. 13 del Codice della Privacy e all'art. 13 del GDPR*».

Conclusione operativa: ogni monitoraggio deve essere documentato, limitato allo scopo, basato su ruoli e autorizzazioni, preceduto – ove dovuto – da informativa e valutazione *privacy*, e sottoposto a verifiche periodiche.

7. KPI, monitoraggi e *stress test*

- Percentuale di protocolli coperti da formazione e tasso di completamento per funzione.
- Percentuale di processi auditati, rilievi chiusi entro SLA (help desk) e tempi medi di *remediation*.
- Numero, tipologia e tempi di gestione delle segnalazioni *whistleblowing*.
- Percentuale di incidenti cyber gestiti secondo *playbook* e tempi di *escalation*/notifica.
- Copertura dell'inventario IA, esiti dei controlli sui fornitori e anomalie rilevate dai sistemi di monitoraggio.
- Analisi degli scostamenti rispetto a *budget*, obiettivi, perdite, *performance* e guadagni; stress test periodici sui processi sensibili.

L'uso dell'IA nei controlli deve essere assistito da supervisione umana: un *alert* non sostituisce la decisione, ma abilita blocchi, verifiche, escalation e registrazioni tracciabili.

8. Incentivi fiscali: quadro vigente e misure in esaurimento

Dal 1° gennaio 2026, il credito d'imposta per investimenti in beni strumentali 4.0 e il Piano Transizione 5.0 non sono più operativi e sono sostituiti dall'iperammortamento di cui all'art. 1, commi 427-436, L. 30 dicembre 2025, n. 199, modificato dal D.L. 27 marzo 2026, n. 38, convertito dalla L. 22 maggio 2026, n. 88, con decreto interministeriale attuativo del 7 maggio 2026: la misura opera come maggiorazione del costo fiscalmente deducibile per gli investimenti effettuati dal 1° gennaio 2026 al 30 settembre 2028. Per i

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

soggetti ISA che aderiscono al concordato preventivo biennale, la L. 22 maggio 2026, n. 88 ha previsto che la maggiorazione delle quote di ammortamento e dei canoni di leasing non rilevi nella determinazione del reddito oggetto di concordato, con una corrispondente variazione di quest'ultimo. Con riferimento alla Transizione 5.0, residuano le sole posizioni prenotate sulla piattaforma GSE entro il 27 novembre 2025, oltre alla misura compensativa riconosciuta alle imprese rimaste escluse per esaurimento delle risorse. Restano disponibili, secondo disciplina vigente e condizioni applicabili, il credito d'imposta ricerca e sviluppo, innovazione e design, il Patent Box di cui all'art. 6 D.L. 146/2021, la ZES Unica e la Nuova Sabatini. Il credito d'imposta Formazione 4.0 non è applicabile alle spese sostenute dopo il 31 dicembre 2022.

Un aspetto merita di essere valorizzato, perché incide sulla convenienza dell'adeguamento. Non tutte le spese sostenute per conformarsi alle normative qui esaminate hanno lo stesso trattamento fiscale, e distinguerle è la prima cosa da fare. I costi di servizio – consulenza, gap analysis, audit, redazione di procedure, formazione – restano costi d'esercizio, deducibili per competenza ai sensi dell'art. 109 TUIR ma non agevolabili in via ulteriore; lo stesso vale, di regola, per il credito ricerca e sviluppo, che presuppone un'attività realmente innovativa e non il semplice adeguamento normativo.

È invece sul versante degli investimenti in beni strumentali che l'adeguamento può tradursi in un risparmio concreto. In particolare, gli investimenti che l'impresa affronta per adeguarsi alla NIS2 e all'AI Act – sistemi di sicurezza informatica, infrastrutture, hardware e software con licenza acquisiti e capitalizzati – possono accedere all'iperammortamento, beneficiando della maggiorazione del costo deducibile. Il vantaggio non è però automatico: il bene deve rientrare negli allegati di legge, risultare interconnesso ai processi aziendali e seguire la procedura di comunicazione al GSE, da avviare prima dell'ordine. Restano fuori, di norma, i servizi acquistati in abbonamento, come le soluzioni fornite in modalità *software as a service* (*saas*), che non danno luogo a un bene ammortizzabile. Per gli altri adempimenti trattati in questa circolare – dal Modello 231 al whistleblowing, dalla rendicontazione di sostenibilità alla protezione dei dati – il beneficio fiscale è di norma circoscritto alla deducibilità ordinaria dei relativi costi.

Aliquote, massimali, finestre temporali, cumulabilità, comunicazioni e certificazioni sono soggetti a modifiche normative e di prassi; occorre quindi una verifica preventiva tecnico-fiscale sul singolo progetto.

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

9. Linee guida e standard di riferimento

- Linee guida Confindustria e linee guida delle associazioni di categoria per MOG 231.
- *Framework* Nazionale *Cybersecurity* & *Data Protection* (CIS/CINI/ACN, ed. 2025) e determinazioni ACN, da ultimo la n. 379907 del 19 dicembre 2025, da ultimo aggiornata dalla determinazione ACN n. 314287/2026, applicabile dal 25 ottobre 2026, e i successivi aggiornamenti.
- Linee guida EDPB su dark patterns e data breach.
- Linee guida ANAC in materia di whistleblowing.
- UNI-INAIL, ISO 45001 e altre certificazioni pertinenti per i sistemi di gestione della salute e sicurezza.

10. *Check-list* operativa

1. Deliberare l'adozione o l'aggiornamento del MOG e nominare un OdV effettivamente indipendente, con *budget*, *action plan* annuale e flussi informativi formalizzati.
2. Eseguire un *risk assesment* integrato e una *gap analysis* con annesso *remediation plan*; definire priorità, funzioni responsabili delle azioni, scadenze e formazione mirata, individuare eventuali *focal point* per i flussi informativi all'OdV.
3. Aggiornare la *policy whistleblowing*: canali conformi, SLA di 7 giorni e 3 mesi, segregazione degli accessi, registro delle attività e raccordo con OdV.
4. Per GDPR: verificare informative *layered*, assenza di dark patterns, DPIA per trattamenti ad alto rischio e piano di gestione dei *data breach*.
5. Per NIS2: verificare la qualificazione dell'ente, confermare la registrazione sul portale ACN nella finestra annuale 1° gennaio – 28 febbraio, nominare il Referente CSIRT e il sostituto, adottare le misure di sicurezza di base nei termini della determinazione ACN n. 379907/2025, definire il processo di notifica degli incidenti e presidiare la *supply chain*.
6. Per AI Act: completare inventario e classificazione dei sistemi di IA; verificare gli obblighi applicabili in funzione del ruolo di *provider/deployer*; verificare l'assolvimento degli obblighi di trasparenza ex art. 50, applicabili dal 2 agosto 2026, e della marcatura ex art. 50, par. 2, dovuta dal 2 dicembre 2026 per i sistemi già immessi sul mercato;

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

programmare l'adeguamento ai requisiti dell'alto rischio secondo il calendario differito al 2 dicembre 2027 e al 2 agosto 2028.

7. Per CSRD/ESRS: verificare la collocazione dell'impresa nel calendario risultante dalla Dir. (UE) 2025/794 e dalla L. 118/2025, quindi definire la *governance* ESG, l'analisi di doppia materialità, i controlli interni e i flussi informativi all'OdV.

Priorità: avviare un *assesment* unitario SG&II, superando una gestione frammentata dei diversi adempimenti; la coerenza tra *governanc*e, dati, sicurezza, persone e tecnologia rappresenta, infatti, il presupposto fondamentale per un'efficace prevenzione e gestione dei rischi.

11. Allegato – Matrice "Reati 231 × Controlli/Procedure" (estratto aggiornato)

Funzione	231	Presidi SG&II	KPI / raccordi
Acquisti	24, 25, 25-*octies*, 25 *octies*.2, 25-*undecies*	*Due diligence* fornitori; segregazione poteri; tracciabilità; controlli EHS; clausole *cyber* e IA.	*Vendor rating*; NIS2 *supply chain*; GDPR
Vendite / *Marketing*	24, 25-*bis*, 25-*bis.*1, 25-*terdecies,* 25 *octies.2*	Approvazione prezzi; tutela *brand*/IP; *policy* comunicazione; trasparenza dei contenuti IA; due diligenze clienti se si opera su mercati internazionali	Reclami; controlli art. 50 AI Act; GDPR
IT / *Security*	24-*bis*, 25-*novies, 25-vicies*	IAM; *patching*; *logging*; *software asset management*; *incident response*; inventario AI.	Incidenti e *remediation*; NIS2; AI Act
Finance	25-ter, 25-*sexies*, 25-*octies*, 25-*octies*.1, 25 octies.2, 25-*quinquiesdecies*	Controlli contabili; KYC/AML; riconciliazioni; verifica di inerenza ed effettività delle operazioni; controlli su crediti d'imposta e compensazioni; autorizzazioni e flussi tracciati.	Eccezioni; tempi di chiusura; presidi 231 e reati tributari

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)

HSE	25-*septies*, 25-*undecies*	SGSL art. 30; manutenzioni; *near miss*; autorizzazioni e monitoraggi ambientali.	Infortuni/*near miss*; ISO 45001; ESRS
HR	25-*quinquies*, 25-*duodecies*, 25-*terdecies*	DEI *policy*; verifiche documentali; formazione; controlli proporzionati; *whistleblowing*.	Formazione; segnalazioni; GDPR / CEDU

Nota metodologica. La matrice è un estratto orientativo e deve essere completata per società, processi, sedi, deleghe, applicativi, fornitori e fattispecie di rischio concretamente rilevanti. La matrice non costituisce un elenco esaustivo dei reati presupposto né sostituisce il *risk assessment* specifico dell'ente.

Milano – Roma, 12 novembre 2026

VITTORIO EMANUELE FALSITTA & PARTNERS S.p.A.
Cod. Fisc./Partita Iva IT11617840969 • Registro Imprese di Milano C.C.I.A.A. • R.E.A. n. MI-2615092
falsitta@falsitta.it • PEC vefpartners@legalmail.it
Other working languages: Arabic • English • French

ANDREANO STUDIO LEGALE S.t.A.
Cap. Soc. € 105.429,00 • REA RM-1486302 • C.F./P.IVA 02297030427
studiolegaleandreano.it • studioandreano@pec.it
Correspondent offices: EuropAfricAsiAmerica

Circolare Informativa in sigla SG&II. Sicurezza Giuridica & Informatica Integrata. Studio Falsitta/Andreano. Tutti i diritti riservati. (revisione novembre 2026)