BIELLE CONSULTING

Risk, Sustainability & Compliance

Bielle Consulting – Governance, Risk & Compliance Newsletter

N.5 · MAGGIO 2026

La newsletter mensile di riferimento per Board, Legal Counsel e Compliance Officer su normativa, giurisprudenza e rischi d'impresa.

Indice

I. Executive Summary

Ad aprile 2026, l'ecosistema normativo e giurisprudenziale impone un immediato riposizionamento strategico, ridisegnando le architetture di responsabilità penale e amministrativa degli enti. Di seguito le priorità assolute per il Board:

Privacy e Prevenzione Frodi (Caso Poste)

Maxi-sanzione di 12,5 milioni di euro dal Garante Privacy per le illecite pratiche di scansione massiva dei dispositivi tramite app. Le direttive europee sui pagamenti digitali (PSD2) non costituiscono un'esimente per aggirare la privacy accountability.

Stretta Antitrust (AGCM)

A valle del record storico di 1,4 miliardi di euro di sanzioni irrogate nel 2025, ad aprile l'Autorità ha colpito con oltre 23,2 milioni di euro un cartello storico nella fornitura di snack per la GDO e ha sanzionato per 3 milioni i Materassi Marion per pratiche commerciali scorrette e ingannevoli.

Estensione del Rischio Caporalato

La Corte di Cassazione (sent. 12685/2026) sdogana l'applicabilità del reato di sfruttamento della manodopera anche al settore dei servizi e del terziario, ampliando drasticamente i rischi per chi esternalizza servizi.

Nuovi Reati 231 Agroalimentari

L'approvazione definitiva del DDL a tutela dei prodotti alimentari italiani introduce nuove fattispecie come la "frode alimentare" nel catalogo dei reati presupposto, richiedendo una revisione d'emergenza dei Modelli Organizzativi per l'intera filiera food & beverage.

Sanzioni Penali sullo Smart Working

L'entrata in vigore della Legge 34/2026 (7 aprile 2026) punisce con l'arresto fino a quattro mesi la mancata consegna dell'informativa scritta sui rischi specifici del lavoro agile a datori di lavoro e dirigenti.

Governance e Cyber Security (TUFe NIS2)

Entra in vigore la riforma della Corporate Governance (D.Lgs. 47/2026) con impatti diretti sui mercati dei capitali. Contestualmente, l'ACN fissa scadenze inderogabili per la conformità NIS2: 31 maggio (censimento dei fornitori rilevanti) e 30 giugno (categorizzazione dei servizi aziendali).

Rischi 231 su Fondi Pubblici e Sequestri

La truffa sul Superbonus legittima la confisca sia del credito fiscale sia del profitto (Cass. 11608/2026). Di contro, la Cassazione offre uno scudo difensivo (sent. 13414/2026) obbligando il GIP a motivare autonomamente il vantaggio dell'ente per i sequestri preventivi, disinnescando gli automatismi sanzionatori.

II. IL FATTO DEL MESE: Il "Caso Poste" e il Limite dell'Invasività Tecnologica

Il 17 aprile 2026, il Garante per la protezione dei dati personali ha emesso il provvedimento n. 237/2026, colpendo le architetture tecnologiche del principale operatore postale e finanziario italiano. Le sanzioni irrogate, per un totale di **12.501.000** euro (ripartite in **6.624.000** euro per Poste Italiane S.p.a. e **5.877.000** euro per PostePay S.p.a.), derivano da accertamenti su pratiche di trattamento dati giudicate massivamente illecite, eseguite tramite le applicazioni BancoPosta e PostePay su sistemi operativi Android.

L'indagine ha focalizzato l'attenzione sull'utilizzo di *Software Development Kit (SDK)* di terze parti, integrati con l'obiettivo di analizzare la *device reputation*, ossia l'affidabilità del dispositivo, monitorando le abitudini di utilizzo, l'elenco delle applicazioni installate sul terminale, e l'eventuale presenza di software malevoli.

€ 6.624.000
Sanzione Poste Italiane S.p.A.

€ 5.877.000
Sanzione PostePay S.p.A.

Il Crollo dell'Impianto Difensivo: PSD2 e Base Giuridica

L'elemento di maggiore rilevanza risiede nella meticolosa decostruzione, operata dal Garante, dell'impianto difensivo basato sull'adempimento di obblighi normativi. Le società contitolari hanno tentato di fondare la legittimità della scansione massiva sull'obbligo legale derivante dalla Direttiva europea sui servizi di pagamento (PSD2) e dai relativi standard tecnici emanati dall'Autorità Bancaria Europea (EBA).

L'Autorità ha statuito che tali direttive non prescrivono né autorizzano in alcun modo una scansione indiscriminata dei terminali degli utenti. L'accesso a informazioni archiviate nell'apparecchiatura terminale ricade nell'ambito di applicazione dell'articolo 122 del Codice della Privacy, il quale esige il consenso preventivo, libero e informato dell'utente.

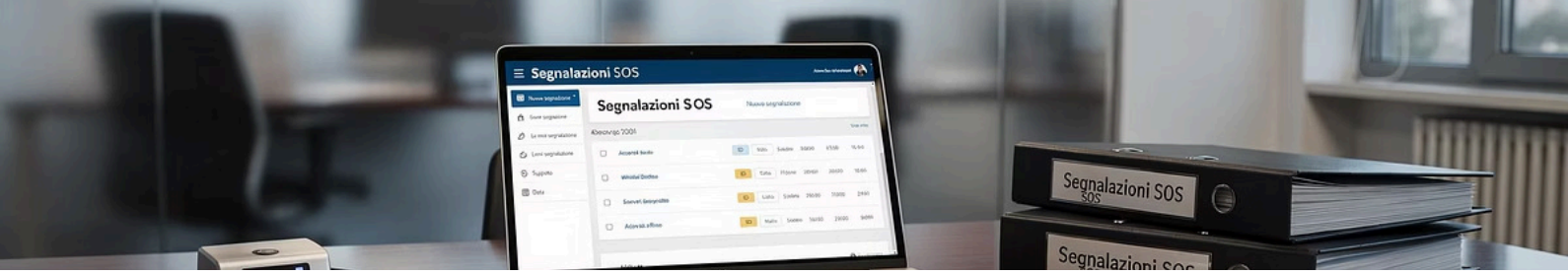
Un ulteriore tentativo di difesa si è basato sull'utilizzo di tecniche crittografiche (funzione di hashing MD5), rigettato perché tale conversione non garantisce un'anonimizzazione assoluta, ma una mera pseudo-anonimizzazione. La mancata redazione di una Valutazione d'Impatto (DPIA) è stata giudicata una violazione gravissima. Infine, il provvedimento ha censurato le dinamiche di *take-it-or-leave-it*: bloccare l'uso dell'app dopo tre rifiuti di autorizzazione priva il consenso della sua libertà, rendendolo nullo.

PSD2
Non prescrive né autorizza scansioni indiscriminate dei terminali

Hashing MD5
Garantisce solo pseudo-anonimizzazione, non anonimizzazione assoluta

Take-it-or-leave-it
Bloccare l'app dopo 3 rifiuti priva il consenso della sua libertà

Messaggio Strategico per il Board: L'implementazione di tecnologie di *fraud management* non gode di salvacondotti normativi. I Consigli di Amministrazione devono esigere che venga valutata preventivamente (tramite DPIA documentate) ogni interazione con i dispositivi personali degli utenti. Qualsiasi prassi che condizioni l'erogazione del servizio principale alla cessione di dati eccedenti costituisce un rischio di compliance non calcolabile.



III. Agenda Authority e Sanzioni: Focus su Antitrust, Antiriciclaggio e Whistleblowing

1. Antitrust (AGCM): Record Storico e Tolleranza Zero su Cartelli e Marketing Scorretto

Ad aprile 2026, la pubblicazione della Relazione Annuale dell'AGCM ha messo in luce la straordinaria pressione esercitata dall'Autorità: nel solo anno 2025, le sanzioni irrogate hanno raggiunto il record storico di **1,4 miliardi di euro**. Questa tendenza si è immediatamente riflessa nei provvedimenti del mese.

Il 28 aprile 2026, l'AGCM ha chiuso un'importante istruttoria sanzionando per complessivi **23.298.147 euro** i produttori Amica Chips S.p.A., Pata S.p.A. e Preziosi Food S.p.A.. L'indagine ha svelato un'intesa segreta finalizzata a eludere le logiche competitive nelle forniture alla GDO (mercato delle private label). Le aziende si sono rese protagoniste di una ripartizione sistematica dei volumi, orchestrando strategie di offerte di comodo e concordando incrementi tariffari ingiustificati. Per abbattere le sanzioni, è stato utilizzato congiuntamente il Programma di Clemenza e, per la prima volta nella storia dell'Autorità, la nuova procedura di transazione (settlement).

Sempre ad aprile, il rigore dell'Antitrust ha colpito il versante della tutela del consumatore, comminando una sanzione di **3 milioni di euro** alla Emme Group S.p.A. (Materassi Marion). La condanna è derivata dall'accertamento di pratiche commerciali scorrette e aggressive: l'azienda utilizzava televendite ingannevoli per promuovere sconti fittizi, inducendo in un secondo momento i consumatori – spesso anziani – all'acquisto a domicilio di varianti di prodotto molto più costose tramite indebite pressioni psicologiche.

€ 1,4 miliardi
Record storico sanzioni AGCM 2025

€ 23.298.147
Sanzione cartello snack GDO (aprile 2026)

2. Antiriciclaggio (UIF): Nuove Mappe del Crimine e Abusi sui Fondi PNRR

Il 20 aprile 2026, l'Unità di Informazione Finanziaria per l'Italia (UIF) ha pubblicato il **"Quaderno n. 34 sulle Casistiche di riciclaggio e di finanziamento del terrorismo"**. La UIF lancia l'allarme sull'evoluzione strutturale dei network criminali, che hanno abbandonato i metodi rudimentali in favore del cosiddetto **"Money Laundering as a Service" (MLaaS)**. Il Quaderno evidenzia un aumento sistematico dei flussi finanziari di provenienza illecita inviati verso Paesi del Sud-Est asiatico tramite l'uso di servizi di Virtual IBAN forniti da Payment Service Providers (PSP) esteri.

L'altro grande filone di rischio riguarda l'abuso dei fondi comunitari (ad esempio nel comparto agricolo) e dei bonus edilizi/PNRR, orchestrate tramite l'interposizione di fiduciarie e la distorsione di contratti di escrow per garantire l'illecita circolazione dei crediti fiscali. A supporto, la UIF ha imposto l'utilizzo di nuovi codici per le Segnalazioni di Operazioni Sospette (SOS): **PA1** (Abusi su agevolazioni pubbliche) e **PA2** (Abusi relativi a contratti pubblici).

PA1
Abusi su agevolazioni pubbliche

PA2
Abusi relativi a contratti pubblici

3. Vademecum ANAC sul Whistleblowing: La Fine del Fai-da-Te

Ad aprile 2026 è emerso con forza il peso delle Linee Guida ANAC emanate tramite le delibere 478 e 479, ora supportate dai vademecum operativi di Assonime. Le direttive impongono adeguamenti tecnici stringenti:

1. Obbligo di Piattaforme Crittografate: Viene sancito che l'utilizzo della posta elettronica ordinaria o della PEC è, di default, inidoneo a garantire la riservatezza, tollerato solo previa DPIA e specifiche motivazioni.
2. Gruppi Societari e Outsourcing: La condivisione della medesima piattaforma interna tra società del gruppo è ammessa esclusivamente se tutte le controllate possiedono meno di 249 dipendenti. Se una lo supera, diviene obbligatoria l'esternalizzazione (outsourcing) a un soggetto terzo indipendente.
3. Il Vincolo Sindacale: L'implementazione del canale interno impone un coinvolgimento preventivo delle rappresentanze sindacali. Omettere l'informativa sindacale espone la società a sanzioni ex art. 21 del D.Lgs. 24/2023 (fino a 50.000 euro).

IV. Governance, Nuova Legislazione e Cyber Security: Riforma TUF, DDL Agroalimentare, Sicurezza sul Lavoro e Direttrici NIS2

La Rivoluzione della Governance Societaria: Il D.Lgs. 47/2026

Il 14 aprile 2026 è stato pubblicato il D.Lgs. 27 marzo 2026, n. 47 (attuativo della Legge Capitali), entrato in vigore il 29 aprile. Questo provvedimento interviene chirurgicamente sul TUF e sul Codice Civile per colmare il divario di competitività del mercato italiano.

Per i Consigli di Amministrazione, le implicazioni di adeguamento sono immediate:

- Flussi Informativi e Responsabilità: La riforma esplicita che l'efficacia della governance non è statica. Viene rafforzata la responsabilità degli amministratori per l'inadeguatezza dei flussi informativi sui rischi sistemici.
- Le Società di Partenariato: Viene forgiato un nuovo veicolo giuridico, la "società di partenariato", modellata come OICR chiuso in accomandita per azioni, finalizzata a captare risorse verso private equity e venture capital.
- Evoluzione OPA e Aggregazioni: Si abroga il divieto di interlocking directorates nei mercati finanziari e si introduce il meccanismo dell'"acquisto totalitario su autorizzazione dei soci" per evitare un'OPA basta il voto favorevole del 75% del capitale dei presenti comprensivo del 50% +1 del capitale delle minoranze indipendenti presenti.

Il DDL Agroalimentare: Nuovi Reati e Ampliamento del Catalogo 231

Il 15 aprile 2026, il Parlamento ha approvato in via definitiva il Disegno di Legge recante "Disposizioni sanzionatorie a tutela dei prodotti alimentari italiani". Il testo rivoluziona il quadro penalistico introducendo nel Titolo VIII del Codice Penale il nuovo Capo II-bis, specificamente dedicato ai "Delitti contro il patrimonio agroalimentare". Oltre ad inasprire le pene e prevedere confische o chiusure degli stabilimenti, il provvedimento conia nuove fattispecie autonome, tra cui spicca la "frode alimentare" (art. 517-sexies c.p.) e il "commercio di alimenti con segni mendaci" (art. 517-septies c.p.).

Di vitale importanza per i Board è l'impatto sistemico sulla compliance: la normativa modifica l'art. 25-bis.1 del D.Lgs. 231/01 (Delitti contro l'industria e il commercio), inserendo formalmente i nuovi reati nel catalogo dei reati presupposto dell'ente. Ciò rende l'adeguamento del Modello 231 un imperativo improrogabile per tutte le società del settore agricolo, della GDO, della logistica e della produzione alimentare, al fine di evitare le pesanti sanzioni interdittive e pecuniarie previste.

Art. 517-sexies c.p.
Frode alimentare

Art. 517-septies c.p.
Commercio di alimenti con segni mendaci

Sicurezza sul Lavoro: Sanzioni Penali per lo Smart Working e MOG Semplificati (Legge 34/2026)

La Legge 11 marzo 2026, n. 34 (in vigore dal 7 aprile 2026) introduce gravosi presidi sanzionatori per la sicurezza sul lavoro. Sotto il profilo del lavoro agile, la modifica dell'Art. 55 del D.Lgs. 81/08 introduce l'arresto da 2 a 4 mesi (o ammenda fino a **€7.403**) per il datore di lavoro e il dirigente che omettano di consegnare al lavoratore e all'RLS, con cadenza almeno annuale, l'informativa scritta sui rischi generali e specifici dello smart working. Viene introdotto, altresì, l'obbligo di formazione sulla sicurezza per i dipendenti posti in **Cassa Integrazione Guadagni (CIG)**. Contestualmente, la normativa interviene in un'ottica di proporzionalità e semplificazione organizzativa, incaricando formalmente l'INAIL di elaborare nuovi **Modelli di Organizzazione e Gestione (MOG) semplificati** destinati alle PMI, con l'obiettivo di agevolare l'esenzione dalla responsabilità amministrativa (ex D.Lgs. 231/01) limitando il peso degli oneri burocratici documentali a carico delle realtà di minori dimensioni.

Direttiva NIS2: Le Nuove Scadenze ACN per Maggio e Giugno

Sul fronte della sicurezza informatica, il mese ha registrato una fortissima accelerazione. L'Agenzia per la Cybersicurezza Nazionale (ACN) ha pubblicato tramite apposite determinazioni le Linee Guida e le scadenze inderogabili per il nuovo modello di categorizzazione delle attività (Det. 155238/2026).

I Chief Information Security Officer (CISO) sono chiamati a rispettare due date cruciali:

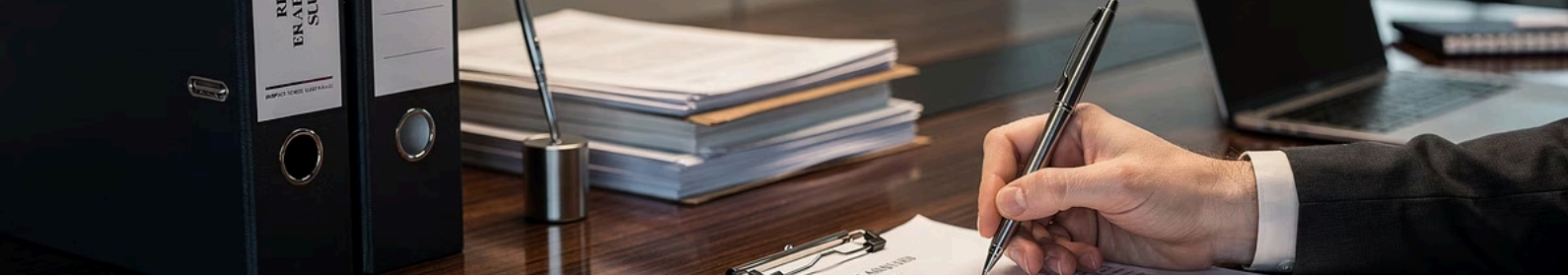
1. 31 Maggio 2026: Entro questa data, tutti i soggetti NIS devono obbligatoriamente interrogare la piattaforma ACN e censire i propri "fornitori rilevanti". Questo adempimento colpisce la supply chain tecnologica, obbligando all'identificazione dei fornitori IT "infungibili" la cui compromissione paralizzerebbe l'operatività dell'ente.
2. 30 Giugno 2026: Termine ultimo per completare, sempre sulla piattaforma ACN, la formale categorizzazione delle proprie attività e dei servizi suddividendoli in 10 macro-aree e 4 livelli di impatto. Sbagliare questa fase espone l'ente all'assegnazione di misure di sicurezza errate nel lungo termine e a un conseguente vuoto di conformità penale e amministrativa.

31 Maggio 2026
Censimento fornitori rilevanti sulla piattaforma ACN

30 Giugno 2026
Categorizzazione attività e servizi (10 macro-aree, 4 livelli di impatto)

Orizzonti ESG: Rating Extra-UE e Ridimensionamento della CSRD

Il 29 aprile 2026, l'ESMA ha pubblicato le linee guida sull'endorsement dei **Rating ESG**, che stabiliscono regole draconiane (operative da luglio 2026) per consentire ai fornitori europei di avallare valutazioni provenienti da agenzie allocate fuori dall'UE. Sul versante CSRD, l'approvazione del pacchetto "Omnibus I" cancella l'obbligo imminente di *reasonable assurance* (sicurezza ragionevole) in favore della sola *limited assurance* (sicurezza limitata) per i bilanci di sostenibilità, alleggerendo temporaneamente l'onere documentale per le imprese fino al **2027**.



V. Giurisprudenza e Sicurezza: Caporalato, Superbonus e Sequestri

Sent. 12685/2026 — 7 Aprile
Caporalato esteso ai servizi e al terziario

Sent. 13414/2026
Scudo difensivo: GIP deve motivare autonomamente il vantaggio dell'ente

1 2 3 4

Sent. 11608/2026
Superbonus: confisca del credito fiscale e del profitto

Sent. 8397 e 7563/2026
Autonomia del Modello 231: "risparmio" come vantaggio

1. Applicazione del Reato di Caporalato: Dai Campi ai Servizi Urbani

La sentenza n. 12685 del 7 aprile 2026 della Corte di Cassazione imprime una svolta copernicana nell'interpretazione dell'articolo 603-bis c.p. Il reato di **"caporalato"**, storicamente legato a settori come l'agricoltura e l'edilizia, viene ora applicato anche al settore dei servizi e del terziario. La pronuncia (relativa allo sfruttamento dei benzinai) stabilisce che la **"manodopera"** si riferisce a qualsiasi attività subordinata di natura prevalentemente manuale. Inoltre, i giudici hanno chiarito che lo **"stato di bisogno"** della vittima non deve essere confuso con l'indigenza estrema, essendo sufficiente una grave difficoltà economica transitoria. La combinazione con il recente **Decreto Lavoro** (che combatte il caporalato digitale e l'opacità degli algoritmi) innalza esponenzialmente il rischio 231 per le aziende committenti che esternalizzano servizi.

2. Superbonus e Rischio 231 per le Imprese Edili

Il comparto dei crediti edilizi si consolida quale area di massivo rischio penale e amministrativo. Con la fondamentale sentenza n. 11608/2026, la Suprema Corte ha stabilito che la commissione del delitto di truffa aggravata per il conseguimento di erogazioni pubbliche, ottenuta tramite la creazione di un **Superbonus fraudolento**, legittima il sequestro e la confisca sia del credito fiscale sia del profitto derivante dalla sua cessione a terzi. Per le società operanti nel settore edile, questo pronunciamento impone una revisione urgente del Modello Organizzativo, che deve innalzare le barriere di controllo e la tracciabilità delle asseverazioni tecnico-fiscali.

3. Lo Scudo Difensivo contro i Sequestri Preventivi

Sempre in ambito di responsabilità degli Enti, la sentenza della Cassazione n. 13414/2026 di aprile ha tracciato un importantissimo argine procedurale a favore delle aziende in caso di sequestro cautelare. I giudici di legittimità hanno annullato un sequestro milionario chiarendo che il Giudice per le Indagini Preliminari (GIP) ha l'obbligo di motivare in via autonoma la sussistenza del requisito dell'**"interesse o vantaggio"** dell'ente per disporre il provvedimento. Questa pronuncia stabilisce che l'ente non risponde in via automatica: l'accertamento non può appiattirsi acriticamente sulla descrizione delle condotte illecite dei singoli manager o amministratori infedeli, fornendo così all'azienda un vitale strumento di ricorso formale.

4. Autonomia del Modello 231 e il "Risparmio" come Vantaggio

A chiusura del cerchio giurisprudenziale, le sentenze 8397 e 7563 del 2026 confermano che l'autonoma responsabilità dell'ente sussiste a pieno titolo ogniqualvolta l'omissione delle norme prevenzionistiche (infortuni sul lavoro) derivi da una politica aziendale orientata scientemente al **risparmio sui costi operativi** (DPI, formazione). La **"colpa di organizzazione"** sopravvive persino in caso di prescrizione del reato a carico del manager responsabile.

VI. Azioni Prioritarie Consigliate

Le funzioni aziendali (Legal, Compliance, IT e HR) devono coordinarsi per implementare la seguente checklist operativa.

1

Neutralizzare il Rischio Sanzioni Privacy sulle App (DPIA Urgente):

Avviare un audit tecnico su tutte le applicazioni. Sulla scia del "Caso Poste", è imperativo verificare l'implementazione di SDK di device scanning. Qualsiasi pratica di profilazione tecnica deve essere bloccata in assenza di una DPIA ex art. 35 GDPR, rimuovendo al contempo le interfacce manipolative (take-it-or-leave-it).

2

Revisione Contrattualistica e Marketing B2C (Antitrust):

A fronte del record di sanzioni (1,4 mld di euro nel 2025) e del caso Amica Chips, i General Counsel devono presidiare i contratti di filiera per vietare lo scambio di informazioni sensibili o di ripartizione del mercato. Contestualmente, alla luce del caso Marion, è prioritario effettuare un audit sulle strategie di telemarketing ed e-commerce, assicurandosi della veridicità degli sconti applicati e dell'assenza di pressioni o dark patterns.

3

Adempimenti Imminenti NIS2 ACN (Scadenze Maggio e Giugno):

Le realtà "essenziali o importanti" devono accedere al portale dell'Agenzia per la Cybersicurezza Nazionale e ottemperare a due scadenze ravvicinate: identificare e registrare a sistema l'elenco dei fornitori IT rilevanti entro il 31 maggio 2026. Successivamente, entro il 30 giugno 2026, l'azienda dovrà aver completato e approvato la matrice di categorizzazione dei propri servizi.

4

Audit sui Modelli Whistleblowing (Addio al "Fai da Te"):

A seguito dei vademecum basati sulle linee guida ANAC, è necessario adottare piattaforme crittografate ad hoc. Per i gruppi di imprese, se almeno una controllata supera i 249 dipendenti, è obbligatorio esternalizzare la gestione. Fondamentale convocare preventivamente le rappresentanze sindacali prima di implementare i canali e/o le modifiche agli stessi.

5

Adeguamento Formativo e Informativa Smart Working (Evitare l'Arresto):

Per depotenziare il rischio penale innescato dalla L. 34/2026, datori di lavoro e RSPP devono redigere e far firmare (almeno annualmente) a tutti i collaboratori in lavoro agile e all'RLS l'informativa scritta sui rischi specifici, la cui mancanza configura ora un reato di arresto.

6

Aggiornamento degli Statuti (Riforma TUF):

Le aziende in mercati regolamentati devono valutare l'impatto del D.Lgs. 47/2026, portando all'ordine del giorno dei prossimi CdA l'adeguamento dei flussi informativi e l'analisi dei nuovi meccanismi OPA ("acquisto totalitario su autorizzazione dei soci").

7

Aggiornamento Modello 231 per la Filiera Agroalimentare:

Le società operanti nel settore food & beverage devono avviare un risk assessment urgente sui nuovi illeciti introdotti dal DDL a tutela dei prodotti alimentari italiani (es. "frode alimentare"), aggiornando tempestivamente le procedure preventive del Modello 231.

BIELLE CONSULTING

Risk, Sustainability & Compliance

📍 Sede

Via Thaon di Revel, 21 - 20159 Milano

📪 Email

info@bielleconsulting.com

☎️ Telefono

+39 3481505622 -

+39 3460875317