BIELLE CONSULTING

Risk, Sustainability & Compliance

Bielle Consulting - Governance, Risk & Compliance Newsletter

N.2 Dicembre 2025

I. Executive Summary

Tenendo conto di quanto accaduto nel mese di novembre 2025, per i Consigli di Amministrazione, i CEO e i Responsabili Compliance, l'agenda delle priorità è dettata dalla necessità di garantire la continuità operativa di fronte a tre minacce sistemiche emerse con chiarezza nelle ultime quattro settimane.

1. La Responsabilità di Filiera e l'Evoluzione del Dolo (Caso Tod’s).
L'inchiesta che ha coinvolto il gruppo Tod's ha subito una svolta inaspettata, con la **Procura di Milano che ha riqualificato le contestazioni a carico dei manager da colpose a dolose**, ipotizzando una "cecità intenzionale" di fronte allo sfruttamento del lavoro nella catena di subfornitura, da qui La richiesta di interdittiva pubblicitaria per sei mesi da parte della Procura Milanese

2. La "Gestione della Sicurezza: POS specifico e Rischio Molestie
La gestione della Salute e Sicurezza sul Lavoro è stata investita da una doppia ondata di rigore.
Sul fronte giurisprudenziale, la Corte di Cassazione (Sentenza n. 37984 del 24 novembre 2025) ha bocciato la prassi della documentazione standardizzata: u**n Piano Operativo di Sicurezza (POS) generico, privo di un'analisi dei rischi specifici legati all’area del cantiere, equivale giuridicamente a un'omessa valutazione**.

Sul fronte legislativo, **con l'entrata in vigore delle norme attuative del D.L. 159/2025**, di cui abbiamo già parlato nella nostra precedente newsletter, **la prevenzione delle molestie e della violenza sui luoghi di lavoro entra formalmente tra le "Misure Generali di Tutela" (Art. 15)**: le molestie non sono più solo un problema disciplinare, ma un **rischio da valutare nel DVR**, pena sanzioni penali e amministrative.

3. La Sovranità del Dato: Cybersecurity e Privacy come Barriere all'Ingresso.
L'Agenzia per la Cybersicurezza Nazionale (ACN) ha reso operativi i criteri di premialità negli appalti, introducendo un meccanismo "On/Off" che premia la sovranità digitale della componentistica ICT.
Parallelamente, **il Garante Privacy,** esprimendo un parere sulle Linee Guida ANAC, h**a di fatto ribadito l'inadeguatezza dell'email come canale whistleblowing**, imponendo la crittografia come standard minimo.

In questo scenario, la newsletter di novembre offre un'analisi profonda e operativa, trasformando le sentenze e i provvedimenti in leve strategiche per blindare la *governance* aziendale.

II. IL FATTO DEL MESE → Perimetro 231: La Responsabilità di Filiera (il Caso Tod’s) e Linee Guida CNDCEC per l’OdV

Il D.Lgs. 231/01 si estende ben oltre i confini giuridici della singola società per abbracciare l'intera catena del valore.

1. Il Caso Tod’s: Dall'Omesso Controllo al "Dolo" Manageriale

L’inchiesta in oggetto coinvolge Tod's Spa e i suoi vertici per il reato di caporalato (art. 603-bis c.p.) commesso nella filiera produttiva.

1.1 L'Ipotesi Accusatoria: La "Cecità Intenzionale"

Inizialmente, l'inchiesta si muoveva sul terreno della colpa per omessa vigilanza. Tuttavia, gli

sviluppi di novembre hanno portato la Procura di Milano (PM Storari) a contestare il dolo a tre top manager e la responsabilità amministrativa all'ente per un fatto doloso.
L'accusa si basa su un **elemento probatorio critico**: gli audit interni. Secondo la Procura, i vertici aziendali erano in possesso di r**eport di audit che evidenziavano le condizioni di sfruttamento presso i subfornitori cinesi** (orari di lavoro illegali, dormitori insalubri, paghe irrisorie). **L'aver continuato a ordinare produzione a questi fornitori**, nonostante la conoscenza delle irregolarità, **ha trasformato la negligenza in "cecità intenzionale" o dolo eventuale** (accettazione del rischio).

1.2 Le Misure Cautelari Richieste

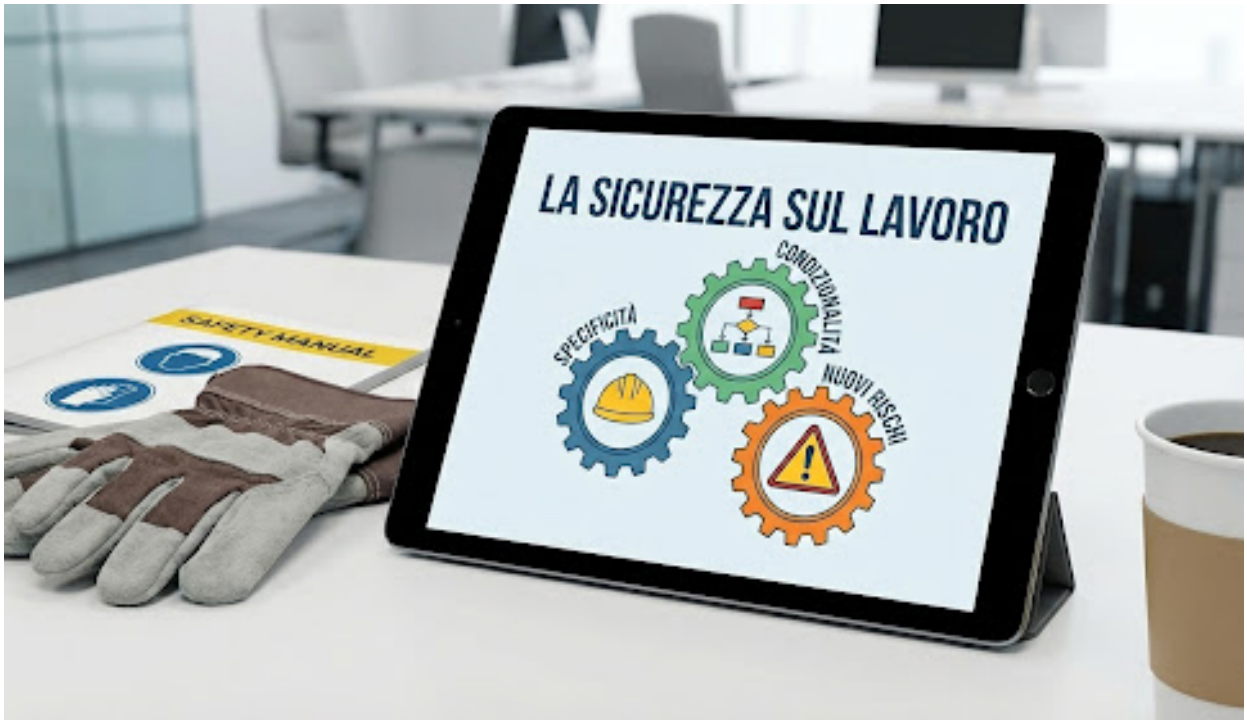
La gravità della situazione è testimoniata dalle misure richieste:

- **Interdittiva Pubblicitaria:** La Procura ha richiesto al GIP **un divieto di pubblicizzare i prodotti per sei mesi.** Una sanzione interdittiva prevista dal Dlgs 231/01 molto rilevante per un brand del lusso operante nel mercato B2C. L'udienza di convalida è prevista per dicembre;
- la Cassazione (udienza 19 novembre) ha respinto le richieste del PM di Amministrazione Giudiziaria (ex art. 34 Codice Antimafia) frequentemente applicata in casi similari.

2. Nuove Linee Guida CNDCEC per l'OdV

Il Consiglio Nazionale dei Dottori Commercialisti ha pubblicato a fine novembre le nuove Linee Guida per l'attività dell'Organismo di Vigilanza. Il documento sottolinea la necessità di superare i controlli meramente documentali, spingendo gli OdV verso l'uso di tecniche di audit sostanziale e *data analytics*.

III. La Sicurezza sul Lavoro tra "Specificità", "Condizionalità" e Nuovi Rischi



1. La Sentenza Cassazione Penale n. 37984/2025: La Fine del POS "Fotocopia"

La sentenza della IV Sezione Penale della Corte di Cassazione n. 37984, depositata il 24 novembre 2025, rappresenta una svolta decisiva per la stesura della documentazione relativa alla sicurezza.

1.1 Il Caso e la Dinamica

La vicenda riguarda un infortunio gravissimo occorso a un lavoratore edile in un cantiere di ristrutturazione a Buja (UD). Il dipendente, intento a rimuovere profili di marmo, è precipitato nel vano ascensore da un'altezza di circa due metri, riportando lesioni midollari permanenti. La difesa del datore di lavoro si fondava su due pilastri:

1. La formale esistenza del Piano Operativo di Sicurezza (POS).
2. L'imprevedibilità della condotta del lavoratore.

La Motivazione della Suprema Corte: Il Principio di Specificità

La Cassazione ha confermato la condanna, smontando le tesi difensive con un ragionamento che impatta direttamente sull'operato di RSPP e Consulenti:

- **L'Inadeguatezza del Documento Generico:** I giudici hanno rilevato che il **POS presentato era "generico" e privo di riferimenti alla specifica situazione dell'area del cantiere (la presenza della fossa ascensore)**. La Corte ha sancito che un POS redatto con in maniera standardizzata, senza un adattamento sartoriale ai luoghi e alle lavorazioni reali, è come se non esistesse. **Un tale documento si limita infatti a una mera funzione burocratica di "copertura" e non è in grado di adempiere alla fondamentale funzione "preventiva" richiesta dalla normativa.**
- **La Consegna Tardiva:** È emerso che il POS e gli atti di appalto erano stati consegnati in cantiere solo il giorno successivo all'infortunio. Questo elemento temporale è stato dirimente per dimostrare l'assenza di una reale pianificazione della sicurezza.
- **La Misura Tecnica Mancante:** La Corte ha sottolineato che, a fronte di un rischio di caduta in un vano aperto, **la misura preventiva non poteva limitarsi a generiche avvertenze, ma doveva prevedere opere provvisionali specifiche (es. ponteggio o parapetto rigido)**.

---

2. D.L. 159/2025: Le Molestie e la Violenza entrano nel DVR

Una delle novità più rilevanti discusse a novembre riguarda la piena operatività delle modifiche introdotte dal **D.L. 31 ottobre 2025, n. 159** ("Decreto Sicurezza"), che ha riscritto parzialmente l'art. 15 del D.Lgs. 81/08.

2.1 La Modifica Normativa: Art. 15 TUSL

La prevenzione delle **condotte violente e moleste** è stata inserita ufficialmente tra le Misure Generali di Tutela con l'aggiunta della lettera *z-bis*. Questo passaggio normativo ha conseguenze operative immediate:

- **Obbligo di Valutazione: Le molestie** (sessuali, psicologiche, mobbing) e le aggressioni (verbali o fisiche) non sono più considerate solo problematiche relazionali o

giuslavoristiche, ma **veri e propri rischi per la salute (stress lavoro-correlato) e la sicurezza del lavoratore.**

- **Integrazione del DVR:** Il Documento di Valutazione dei Rischi deve essere aggiornato. Non basta più il generico riferimento allo "stress lavoro-correlato"; **è necessario mappare specificamente il rischio di molestie, prevedendo procedure di segnalazione e misure di prevenzione** (es. formazione, codici di condotta, canali di ascolto).
- **Settori a Rischio:** Sebbene la norma sia trasversale, l'attenzione dell'Ispettorato (INL) si concentrerà sui settori a maggior interazione con il pubblico (sanità, front-office, trasporti) e sugli ambienti gerarchici chiusi, dove il rischio molestie si sovrappone a quello psicosociale.

Implicazione Strategica: Un'azienda che oggi non aggiorna il DVR includendo il capitolo "Violenze e Molestie" è sanzionabile in caso di ispezione, indipendentemente dal verificarsi di un evento dannoso. Inoltre, in caso di denuncia per molestie, l'**assenza di tale valutazione nel DVR espone l'azienda e il datore di lavoro a responsabilità amministrative e penali dirette per *culpa in organizzando*.**

---

3. La Sentenza Cassazione Civile n. 30334/2025: Il Confine della "Condotta Abnorme"

Se la sentenza penale ha stretto le maglie della responsabilità, la Cassazione Civile, Sez. Lavoro, con la sentenza n. 30334 del 17 novembre 2025, ha delineato con precisione millimetrica l'unico vero esimente per il datore di lavoro: **il rischio elettivo**, ossia un comportamento abnorme, volontario e arbitrario del lavoratore, estraneo alle finalità produttive e non collegato all'attività lavorativa, che interrompe il nesso di causalità tra lavoro e infortunio.

3.1 I Fatti di Causa

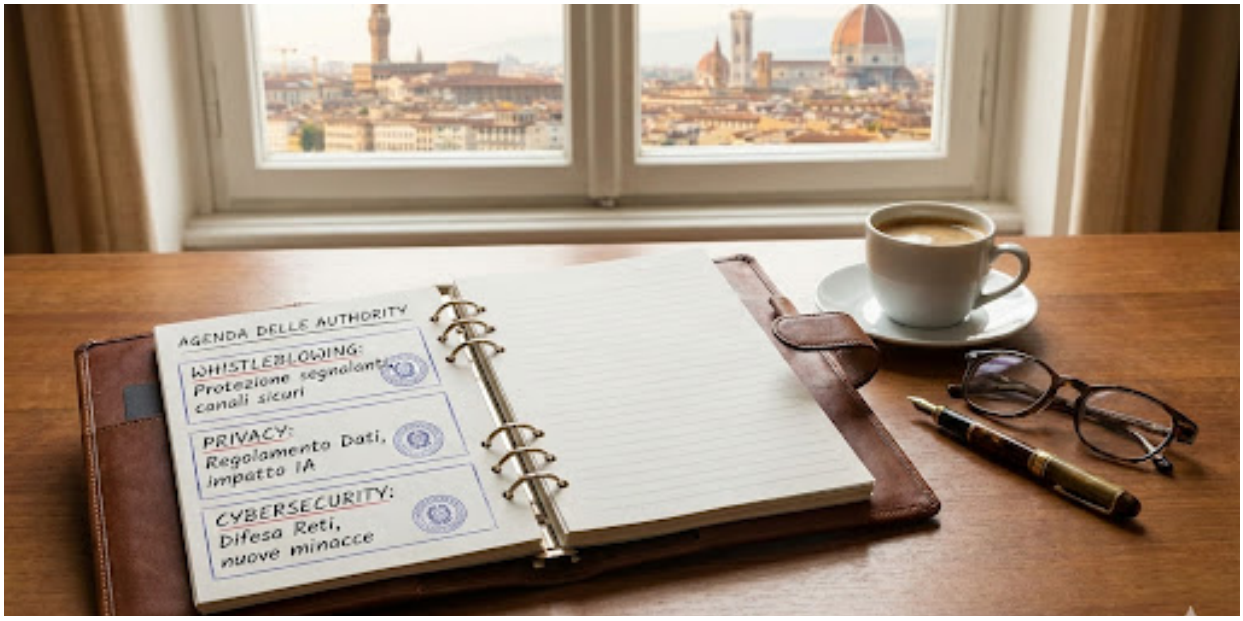
Il caso riguarda un lavoratore (saldatore) che, introdottosi in un'area del cantiere estranea alle sue mansioni e non di proprietà del datore di lavoro, è caduto da una struttura amovibile priva di sicurezza, riportando un'invalidità al 100%. **La Corte d'Appello aveva rigettato la richiesta risarcitoria, ritenendo interrotto il nesso causale.**

3.2 Il Principio di Diritto: L'Imprevedibilità Assoluta

La Suprema Corte ha confermato l'esclusione di responsabilità del datore di lavoro, focalizzandosi sul **concetto di "condotta abnorme":**

- **Estraneità al Processo Produttivo: Il lavoratore** non ha semplicemente agito con negligenza o imprudenza (comportamenti che non esonerano il datore, il quale ha l'obbligo di proteggere il lavoratore anche da se stesso), ma **ha posto in essere una condotta "esorbitante" dalle mansioni affidate.**
- **Il Luogo dell'Evento:** Il fatto che **l'incidente sia avvenuto in un luogo "del tutto estraneo alla prestazione lavorativa" è stato l'elemento chiave**. Il datore di lavoro non può esercitare il potere di controllo e vigilanza in aree che esulano dalla sfera di rischio lavorativo da lui governata.

IV. L'Agenda delle Authority: Whistleblowing, Privacy e Cybersecurity



1. Garante Privacy: "Email inadeguate per le segnalazioni Whistleblowing"

Con il parere del 27 novembre 2025 sugli schemi di Linee Guida ANAC, il Garante Privacy ha sancito la fine dell'epoca "artigianale" nella gestione delle segnalazioni.

1.1. Il Paradosso della Trasparenza e la "Death of Email"

Molte aziende (specialmente PMI) hanno adempiuto all'obbligo di istituire canali di segnalazione creando una semplice casella email (es. *segnalazioni@azienda.it*) accessibile al Gestore delle Segnalazioni. Il Garante Privacy ha sancito che questa modalità è **strutturalmente inadeguata** a garantire la riservatezza dell'identità del segnalante, requisito cardine del D.Lgs. 24/2023.

Il problema risiede nei **metadati**. Anche se il contenuto dell'email è criptato (cosa rara), i log del server di posta registrano inevitabilmente:

- Indirizzo IP del mittente.
- Orario di invio.

- Oggetto e dimensione del messaggio.

Questi dati sono accessibili agli amministratori di sistema (spesso dipendenti dell'azienda stessa o fornitori esterni non segregati), permettendo potenzialmente di risalire all'identità del whistleblower incrociando i log di rete aziendali. Questo rischio di "tracciabilità indiretta" viola l'obbligo di riservatezza assoluta.

1. 2. I Requisiti Tecnologici: Crittografia "At Rest"

Il Garante richiede l'adozione di misure tecniche avanzate, in particolare la **crittografia**.

- **Crittografia del Trasporto e del Contenuto:** Non basta HTTPS. I dati (segnalazione e allegati) devono essere cifrati nel database ("At Rest") con chiavi crittografiche che *non* devono essere nella disponibilità del datore di lavoro o degli amministratori IT aziendali.
- **Segregazione dei Dati:** L'identità del segnalante deve essere conservata in modo separato dal contenuto della segnalazione e accessibile solo al gestore della segnalazione tramite procedure di autenticazione forte.

1.3. Analisi Strategica: Cosa devono fare le aziende?

- **Migrazione a Piattaforme Dedicate:** L'unica soluzione conforme è l'**adozione di piattaforme software specializzate che garantiscano nativamente la crittografia End-to-End e la non tracciabilità dei log** per gli amministratori di sistema.
- **DPIA Obbligatoria: L'adozione del sistema di whistleblowing richiede**, come espressamente previsto dal Dlgs 24/2023 (c.d. Decreto Whistleblowing) una V**alutazione di Impatto sulla Protezione dei Dati (DPIA) specifica**. Il Garante lo ha ribadito: trattandosi di dati potenzialmente giudiziari e di rischio alto per i diritti dei lavoratori (ritorsioni), la DPIA non è opzionale.
- **Gestione dei Canali Vocali:** Anche le segnalazioni orali (linee telefoniche) devono prevedere meccanismi di mascheramento della voce o trascrizione che non conservino la registrazione audio originale accessibile a non autorizzati, per e**vitare il riconoscimento biometrico vocale.**

2. Il Caso "Materiale Istologico": Il Dato è Fisico

Il provvedimento del Garante per la Protezione dei Dati Personali del 9 ottobre 2025, reso pubblico e analizzato nella newsletter di fine novembre, relativo alla vicenda Humanitas

Mirasole S.p.A. offre una casistica perfetta per comprendere come il Regolamento UE 2016/679 (GDPR) penetri nelle pieghe più operative dei processi aziendali.

2.1. Anatomia di un "Data Breach" Biologico

Una paziente, sottoposta a intervento chirurgico per la rimozione di una massa (mucocele), aveva espressamente richiesto **l'esame istologico del tessuto asportato**, nonostante la prassi medica indicasse la natura benigna della lesione e non rendesse l'esame strettamente necessario secondo i protocolli standard. Tuttavia, a causa di un difetto di comunicazione tra il chirurgo e l'infermiere di sala, **il campione prelevato è stato erroneamente smaltito nei rifiuti biologici anziché essere inviato al laboratorio di anatomia patologica**.

Il risultato? Il campione è andato distrutto. Essendo un *unicum* biologico non replicabile, **l'informazione genetica e diagnostica contenuta in quel tessuto è andata persa** per sempre.

2.2. L'Errore di Valutazione del Titolare

La difesa della struttura sanitaria si è basata su una interpretazione tradizionale della privacy, focalizzata sulla **riservatezza**. La società ha sostenuto che, poiché il campione era stato distrutto (smaltito), nessun terzo non autorizzato aveva avuto accesso ai dati della paziente. Non c'era stata esfiltrazione, non c'era stata pubblicazione indebita, non c'era stato furto d'identità. Pertanto, **la struttura ha ritenuto l'incidente a "basso rischio" per i diritti e le libertà dell'interessato e ha deciso di non notificare la violazione al Garante**, limitandosi a informare la paziente e a proporre un percorso di follow-up clinico (risonanze magnetiche periodiche) per monitorare la situazione.

2.3. La Dottrina del Garante: Integrità e Disponibilità

Il Garante ha rigettato con forza questa interpretazione, riaffermando che **la protezione dei dati personali si fonda su tre pilastri interdipendenti (Riservatezza, Integrità, Disponibilità)**. La violazione anche di uno solo di questi parametri costituisce un *Data Breach*.

1. **La Disponibilità come Diritto Fondamentale:** Nel contesto sanitario, la disponibilità del dato (l'esito dell'esame istologico) è precondizione per il diritto alla salute. **La perdita del campione ha privato la paziente di un'informazione essenziale per la sua tranquillità e per la definizione del suo percorso di cura**. Il fatto che la paziente debba ora sottoporsi a controlli radiologici più frequenti e invasivi costituisce, secondo il Garante, un "danno" tangibile derivante dalla violazione privacy.
2. **La Violazione dell'Art. 32 (Sicurezza del Trattamento):** Il Garante ha sanzionato la

struttura per la violazione dell'articolo 32 del GDPR. Nonostante esistessero procedure scritte, l'evento ha dimostrato ch**e le misure tecniche e organizzative non erano efficaci nel mitigare il rischio di errore umano i**n una fase critica come il passaggio di consegne in sala operatoria. La sicurezza "sulla carta" non è sufficiente; i**l sistema deve essere resiliente all'errore del singolo operatore (principio di *Privacy by Design* e tolleranza ai guasti).**

3. **La Violazione dell'Art. 33 (Mancata Notifica): L'omissione della notifica all'Autorità è stata sanzionata autonomamente**. Il Garante ha stabilito che, in presenza di dati relativi alla salute e di un evento irreversibile (distruzione di dato non replicabile), il rischio per l'interessato è intrinsecamente "elevato". **La valutazione di impatto effettuata dal Titolare, che aveva declassato il rischio a "basso", è stata giudicata errata e superficiale**.

2.4. Analisi della Sanzione e Implicazioni Economiche

La sanzione complessiva di **70.000 euro** è stata così ripartita:

- **50.000 euro** per la violazione dei principi di integrità e riservatezza (Art. 5) e delle misure di sicurezza (Art. 32).
- **20.000 euro** per la mancata notifica della violazione all'Autorità di controllo (Art. 33).

Questa ripartizione invia un segnale preciso: **l'errore operativo costa, ma il tentativo di gestire l'incidente "in silenzio", senza coinvolgere l'Autorità, aggrava ulteriormente la sanzione**. La trasparenza, anche nel riconoscimento dei propri errori, è premiata o quantomeno mitiga il danno sanzionatorio.

2.5. Impatti Operativi e Raccomandazioni per le Strutture Sanitarie

Questo provvedimento impone un ripensamento radicale dei processi di *Clinical Risk Management* e della loro integrazione con la Compliance GDPR.

- **Integrazione dei Registri di Rischio:** Non può più esistere un registro degli "eventi avversi sanitari" separato dal registro dei "Data Breach". **Ogni evento clinico che comporta perdita di informazioni** (smarrimento cartelle, perdita campioni, corruzione database immagini, ecc.) **deve attivare simultaneamente i protocolli sanitari e quelli privacy.**
- **Tracciabilità "Fisica" del Dato: Le misure di sicurezza ex Art. 32 devono estendersi alla logistica**. L'uso di tecnologie come barcode o RFID per tracciare i campioni biologici dal momento del prelievo all'arrivo in laboratorio non è più un "nice to have" tecnologico, ma una misura di sicurezza necessaria per dimostrare l' *accountability*.
- **Revisione della Valutazione dei Rischi (DPIA): Le Valutazioni di Impatto** sulla

Protezione dei Dati de**vono includere scenari specifici di "perdita di disponibilità" di dati unici**. Se un dato non ha backup (come un tessuto biologico), il rischio residuo deve essere gestito con procedure di controllo ridondanti (es. "double check" tra due operatori prima dello smaltimento di qualsiasi materiale in sala operatoria).

- **Policy di Notifica:** In caso di dubbio sulla gravità del rischio, **la prudenza impone la notifica al Garante.** La sanzione per mancata notifica è spesso più facile da comminare per l'Autorità (basta verificare le date) rispetto a quella per le misure di sicurezza, che richiede un'istruttoria tecnica complessa.

3. Cybersecurity (ACN): I Criteri di Premialità "On/Off"

Le Linee Guida ACN introducono un meccanismo premiale binario per l'acquisto di ICT, attribuendo:

- **Punteggio ON (8 punti):** Se la **Bill of Material (BOM)** relativa a *tutti* i componenti e servizi di "Livello 1" (critici) indica una provenienza da Paesi UE, NATO o Paesi terzi con accordi di sicurezza specifici (es. White List).
- **Punteggio OFF (0 punti):** Se la **Bill of Material (BOM)** mostra anche un solo componente critico proveniente da un Paese a rischio o non qualificato, il punteggio premiale si azzera.

V. Sostenibilità (ESG): La "Via Volontaria" delle PMI e i Ritardi UE

Nonostante i segnali di rallentamento normativo da Bruxelles (Pacchetto Omnibus), la pressione del mercato sulla sostenibilità non diminuisce.

1. Lo Standard VSME (Voluntary SME)

L'EFRAG ha finalizzato le raccomandazioni per lo standard **VSME** (Voluntary Standard for SMEs). Sebbene formalmente volontario, questo standard è destinato a diventare il linguaggio comune della *Supply Chain*.

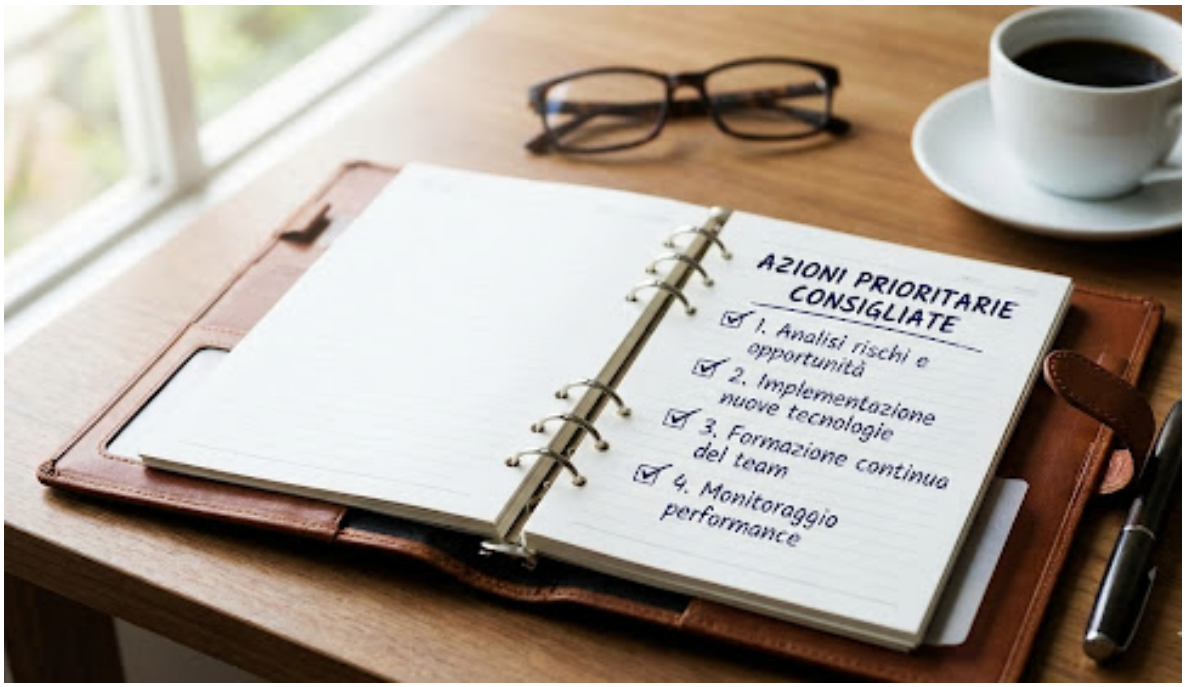
- **L'Effetto Filiera:** Le grandi imprese obbligate alla CSRD d**evono rendicontare le emissioni indirette (Scope 3)** , ovvero quelle prodotte dai loro fornitori **e anche i temi "social" della filiera produttiva**; di conseguenza, stanno iniziando a inviare q**uestionari ESG massivi alle PMI fornitrici.**
- **Standardizzazione:** Lo standard VSME serve a evitare che ogni capofiliera inventi il proprio questionario, creando un caos amministrativo per le PMI. **Adottare il VSME significa produrre un set di dati standardizzato** (moduli "Basic", "Narrative", "Business Partners") **che può essere consegnato a banche e grandi clienti senza dover rifare il lavoro ogni volta**.

2. Il Paradosso dei Rinvii

La Commissione UE ha proposto di rinviare l'adozione degli standard settoriali e di limitare gli obblighi per le aziende extra-UE per "ridurre la burocrazia". Tuttavia il rinvio normativo non ferma le banche.

Gli istituti di credito, vincolati dalle linee guida EBA-LOM, c**ontinuano a integrare i fattori ESG nel merito creditizio.** Un'azienda che, approfittando del rinvio UE, **smette di raccogliere dati ESG, rischia di trovarsi in difficoltà nell'accesso al credito o di pagare spread più alti**. La strategia vincente è anticipare la compliance, usando lo standard VSME come bussola, indipendentemente dai tempi della legislazione europea.

VI. Azioni Prioritarie Consigliate



Alla luce delle evidenze emerse a novembre 2025, Bielle Consulting raccomanda al Top Management e agli organi di controllo l'adozione immediata delle seguenti misure.

1. Supply Chain "Stress Test" (Anti-Caporalato)

- **Obiettivo:** Prevenire misure interdittive (Caso Tod's).
- **Azioni:** Implementare un sistema di valutazione delle terze parti; Identificare i fornitori a rischio non limitandosi alla raccolta documentale: eseguire audit di seconda parte anche "a sorpresa" ed analizzare i risultati per formulare piani di rimedio dettagliati e follow-up.
- **Responsabili:** Direzione Acquisti / Legal / OdV.

2. Audit "Sartoriale" della Documentazione H&S

- **Obiettivo:** Evitare la responsabilità penale per "POS generico" (Cass. 37984/25).
- **Azioni:** Avviare una campagna di audit a campione sui POS e DVR dei cantieri/stabilimenti attivi. Verificare la presenza di elementi specifici (foto, layout, analisi rischi interferenziali reali).
- **Responsabili:** Datore di Lavoro / RSPP.

3. Aggiornamento DVR "Rischio Molestie" (Nuovo D.L. 159/2025)

- **Obiettivo:** Conformità all'art. 15 TUSL e prevenzione responsabilità.
- **Azioni:** Integrare immediatamente il DVR con una sezione dedicata alla valutazione del rischio di violenza e molestie sul lavoro. Istituire una policy interna e programmare formazione specifica per tutto il personale.
- **Responsabili:** RSPP / HR / Datore di Lavoro.

4. Revisione Canale Whistleblowing e DPIA

- **Obiettivo:** Conformità al Parere Garante Privacy e validità delle segnalazioni.
- **Azione:** Dismettere le caselle email dedicate. Implementare piattaforme crittografate (conformi alle Linee Guida ANAC).
- **Responsabile:** Compliance / Gestore delle segnalazioni.

5. Verifica "Bill of Materials" per Appalti ICT

- **Obiettivo:** Accedere ai punteggi premiali ACN (8 punti).
- **Azione:** Utilizzare il tool ACN per analizzare la BOM dei prodotti offerti alla PA e verificare la provenienza geografica: https://developers.italia.it/it/software/dc2dd074-cbac-4abe-9d21-b024b7c0a6a9
- **Responsabile:** CTO / Bid Manager.

Contattateci per ulteriori approfondimenti e per un assessment preliminare!

Studio Bielle Consulting Srl

📍 Via Thaon di Revel, 21 - 20159 Milano

📪 info@bielleconsulting.com

☎️ +39 3481505622 - +39 3460875317