



# BIELLE CONSULTING

Risk, Sustainability & Compliance

## Bielle Consulting – Governance, Risk & Compliance Newsletter

N. 6 · GIUGNO 2026

La newsletter mensile di riferimento per Board, Legal Counsel e Compliance Officer su normativa, giurisprudenza e rischi d'impresa. | Analisi eventi: **maggio 2026**

# Indice

1

**I. Executive Summary – "Le priorità per il CdA"**

2

**II. Il Fatto del Mese: IA che "legge" le emozioni dei dipendenti – il Garante applica per la prima volta il divieto dell'AI Act**

3

**III. Agenda Authority e Sanzioni: Garante Privacy, ACN e NIS2**

4

**IV. Aggiornamenti Normativi e Scadenze Operative: Reati Ambientali 231 e NIS2**

5

**V. Framework e Prassi di Riferimento: CNDCEC Cybersecurity e ESRS/VSME**

6

**VI. Giurisprudenza d'Impresa: DVR e Cancellazione Società**

7

**VII. Azioni Prioritarie Consigliate – "Cosa deve fare il Board oggi"**



# I. Executive Summary – "Le priorità assolute per il CdA"

A maggio 2026, il quadro normativo e giurisprudenziale impone interventi immediati su cinque fronti convergenti: reati ambientali, cybersicurezza, sicurezza sul lavoro, protezione dei dati e intelligenza artificiale applicata al personale.

## Reati ambientali nel 231: catalogo ampliato e sanzioni inasprite

Il **18 maggio 2026** è stato pubblicato il **D.Lgs. 21 aprile 2026, n. 81**, che modifica l'**art. 25-undecies, D.Lgs. 231/2001**. In vigore dal **2 giugno 2026**: nuovi reati-presupposto, quote sanzionatorie più elevate, aggravanti automatiche.

## NIS2: scaduto il 31 maggio l'aggiornamento del Portale ACN

Per i soggetti già iscritti nel 2025, il **31 maggio 2026** era il termine per aggiornare dati e figure responsabili sulla piattaforma ACN. Il rischio è una sanzione fino a **10 milioni di euro o il 2% del fatturato annuo globale** per i soggetti essenziali.

## Sicurezza sul lavoro: il DVR inadeguato condanna datore e RSPP

Con la sentenza **Cass. Pen. Sez. IV n. 16359 del 6 maggio 2026**, la Corte conferma che un *Documento di Valutazione dei Rischi* incompleto comporta la **responsabilità penale** del datore di lavoro e del RSPP.

## Data breach: misure di sicurezza carenti, sanzione del Garante

Il Garante Privacy ha sanzionato **The European House – Ambrosetti S.p.A.** con **85.000 euro** per carenze nelle misure di sicurezza. Norma applicabile: **art. 32 GDPR**

## IA che inferisce le emozioni: primo stop del Garante con l'AI Act

il Garante privacy ha avvertito una *start-up* italiana per un *plug-in* che misura via IA lo stress dei dipendenti, richiamando per la prima volta il divieto dell'**art. 5, par. 1, lett. f) del Reg. (UE) 2024/1689 (AI Act)**, oltre all'**art. 4, legge n. 300/1970** e al GDPR.



## II. Il Fatto del Mese

### IA che "legge" le emozioni dei dipendenti: il Garante applica per la prima volta il divieto dell'AI Act

Con il **provvedimento n. 342 del 14 maggio 2026**, il Garante per la protezione dei dati personali ha rivolto un formale avvertimento a **Myndoor S.r.l.**, *start-up* italiana con sede a Rosate (Milano), che ha sviluppato un *plug-in* per le piattaforme di messaggistica aziendale **Slack e Microsoft Teams**. Lo strumento, basato su *intelligenza artificiale* e analisi semantica delle conversazioni, misura il livello di **stress psicologico** dei lavoratori che scelgono volontariamente di utilizzarlo, restituendo suggerimenti personalizzati per il benessere. L'istruttoria era partita d'ufficio nel **giugno 2025**, dopo notizie di stampa su un possibile impiego anche presso enti della pubblica amministrazione.

Il dato giuridicamente dirompente è il fondamento dell'intervento. Per la prima volta il Garante richiama espressamente l'**art. 5, par. 1, lett. f) del Regolamento (UE) 2024/1689 (AI Act)**, che vieta l'immissione sul mercato, la messa in servizio e l'uso di sistemi di IA destinati a **inferire le emozioni** di una persona fisica nel luogo di lavoro. A questo si aggiungono i limiti del **GDPR** e dell'**art. 4 della legge n. 300/1970** sul controllo a distanza: le informazioni sullo stato emotivo e psicologico dei lavoratori non possono entrare nella disponibilità dell'azienda.

#### Art. 5 AI Act

Vieta sistemi IA per inferire emozioni nel luogo di lavoro

#### Art. 4 L. 300/1970

Limita il controllo a distanza dei lavoratori

#### Art. 32 GDPR

Misure di sicurezza adeguate al rischio del trattamento

Il punto che il Board deve cogliere è la struttura del rischio. Nel caso esaminato il datore di lavoro **non** accedeva né ai contenuti delle chat né ai risultati individuali: titolare del trattamento era la sola società fornitrice. Nonostante questa "distanza", il Garante ha ritenuto comunque illecito il trattamento, per la particolare sensibilità del dato e per il rischio di sorveglianza indiretta. La conseguenza è netta: l'adozione di uno strumento di *wellbeing* basato su IA non è una scelta "tecnica" delegabile al fornitore, ma una decisione di *governance* che impegna la responsabilità dell'impresa cliente.

#### MESSAGGIO PER IL CDA

Il CdA è chiamato a deliberare con urgenza tre interventi:

- **Censire tutti gli strumenti di IA applicati al personale**, già in uso o in valutazione, verificandone la compatibilità con il divieto dell'art. 5 AI Act.
- **Subordinare ogni nuova adozione a una DPIA preventiva** e a un parere di *compliance* congiunto DPO–HR–Legal.
- **Inserire nei contratti con i fornitori di IA** garanzie sulla conformità all'AI Act e sulla titolarità dei trattamenti.



## III. Agenda Authority e Sanzioni

Due fronti hanno scandito l'attività delle Authority nel mese, convergenti su un dato comune: la sicurezza dei dati e dei sistemi è ormai un'area sanzionatoria di prima linea.

### ☒ **Garante Privacy – maggio 2026 – Sanzione: 85.000 euro**

Il Garante ha sanzionato **The European House – Ambrosetti S.p.A.**, società di consulenza strategica e *think tank*, per **carenze nelle misure di sicurezza** emerse a seguito di un *data breach*. La violazione contestata attiene all'inadeguatezza delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, ai sensi dell'**art. 32 del Regolamento (UE) 2016/679**.

⚠ **Impatto pratico per le imprese:** Anche le società di servizi professionali, non solo i grandi titolari, sono esposte; la valutazione del rischio sui sistemi va documentata e aggiornata, non presunta.

### ☒ **ACN – Determinazione n. 127437/2026 – Obbligo per tutti i soggetti NIS**

L'Agenzia per la Cybersicurezza Nazionale ha introdotto, per tutti i soggetti rientranti nel perimetro NIS2, l'obbligo di **elencare i fornitori rilevanti** all'interno della piattaforma ACN, rafforzando il presidio sulla *supply chain security*.

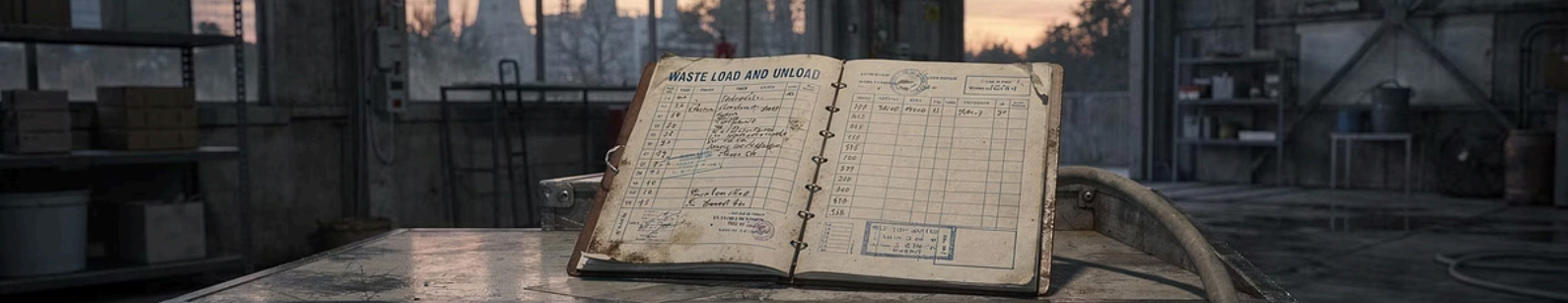
⚠ **Impatto pratico per le imprese:** Gli obblighi NIS2 si trasmettono lungo la catena di fornitura; anche le PMI fornitrici di soggetti essenziali ricevono richieste formali di adeguamento.

**€ 85.000**

Sanzione Garante Privacy — Ambrosetti S.p.A. — maggio 2026

**Det. ACN n. 127437/2026**

Obbligo di censimento fornitori rilevanti sulla piattaforma ACN



## IV. Aggiornamenti Normativi e Scadenze Operative

### Aggiornamento Reati ambientali 231 — D.Lgs. 21 aprile 2026, n. 81 (in vigore dal 2 giugno 2026)

Publicato in **Gazzetta Ufficiale n. 113 del 18 maggio 2026** in attuazione della **Direttiva (UE) 2024/1203**, il decreto interviene sull'**art. 25-undecies, D.Lgs. 231/2001**. Amplia i reati-presupposto — nuova fattispecie di **commercio di prodotti inquinanti (art. 452-bis.1 c.p.)**, modifica dell'**inquinamento ambientale (art. 452-bis c.p.)** — inasprisce le quote sanzionatorie con **aggravanti automatiche (art. 452-sexiesdecies c.p.)** e interviene sull'**art. 256, D.Lgs. 152/2006** (gestione non autorizzata di rifiuti) e introduce i reati su **sostanze lesive dell'ozono e gas fluorurati**. Istituisce inoltre, presso la **Procura Generale della Corte di Cassazione**, un sistema di coordinamento nazionale contro la criminalità ambientale: la pressione investigativa è destinata a crescere. Per gli enti, la *gap analysis* delle aree ambientali del MOG e la *due diligence* su fornitori e gestori di rifiuti non sono più rinviabili.

#### Art. 452-bis.1 c.p.

Nuova fattispecie:  
commercio di prodotti  
inquinanti

#### Art. 452- sexiesdecies c.p.

Aggravanti automatiche —  
inasprimento quote  
sanzionatorie

#### Art. 256, D.Lgs. 152/2006

Gestione non autorizzata di  
rifiuti — norma modificata

## NIS2 — Le scadenze ACN di maggio

Il mese di maggio ha portato a scadenza la fase più operativa dell'attuazione NIS2. Due adempimenti con *deadline* ravvicinate impongono al Board una verifica immediata dello stato di conformità.

#### 31 Maggio 2026

**Aggiornamento del Portale ACN** — I soggetti iscritti nel 2025 dovevano aggiornare informazioni, dati e figure responsabili sulla piattaforma ACN. Mancato adempimento: sanzioni fino a **10 milioni di euro o il 2% del fatturato annuo globale** per i soggetti essenziali.

#### 1° maggio – 30 giugno 2026

**Categorizzazione attività e servizi** — Tramite il nuovo *Servizio* *NIS/Categorizzazione*, i soggetti NIS devono completare la classificazione delle proprie attività e servizi: presupposto per la fase successiva di obblighi proporzionati.

#### 31 Ottobre 2026

**Misure di sicurezza di base** — Termine per il completamento dell'adozione delle misure di sicurezza di base per i soggetti già nel perimetro. Oltre tale data, l'ACN può avviare le attività ispettive.



## V. Framework e Prassi di Riferimento

Due pubblicazioni del mese mettono a disposizione del Board strumenti operativi immediati, su *cyber-compliance* e su sostenibilità.

### ☒ **CNDCEC — "Cybersecurity e Modello 231" (Informativa n. 88 del 18 maggio 2026)**

Il Consiglio Nazionale dei Dottori Commercialisti integra il rischio informatico nei sistemi di *governance*, controllo interno e *compliance*, analizzando i reati informatici rilevanti ai fini 231 — tra cui l'**accesso abusivo a sistema informatico (art. 615-ter c.p.)** — l'impatto dell'*intelligenza artificiale* sulle aree sensibili e il ruolo dell'OdV, anche alla luce della **legge n. 90/2024** sulla cybersicurezza nazionale.

- 📘 **Impatto pratico per le imprese:** È una base metodologica utile per aggiornare il MOG sul rischio *cyber* e per ridisegnare i flussi verso l'Organismo di Vigilanza.

### ☒ **Commissione UE — Consultazione su Revised ESRS e standard VSME (6 maggio 2026)**

La Commissione ha posto in consultazione, fino al **3 giugno 2026**, le bozze finali di due atti delegati: gli *ESRS semplificati* (con riduzione dei *datapoint* obbligatori) e lo standard volontario **VSME** destinato alle imprese non soggette agli obblighi CSRD.

- 📘 **Impatto pratico per le imprese:** Rileva per chi prepara la rendicontazione di sostenibilità e per le PMI che ricevono richieste di dati ESG lungo la *supply chain* dai clienti maggiori.

#### **Informativa CNDCEC n. 88/2026**

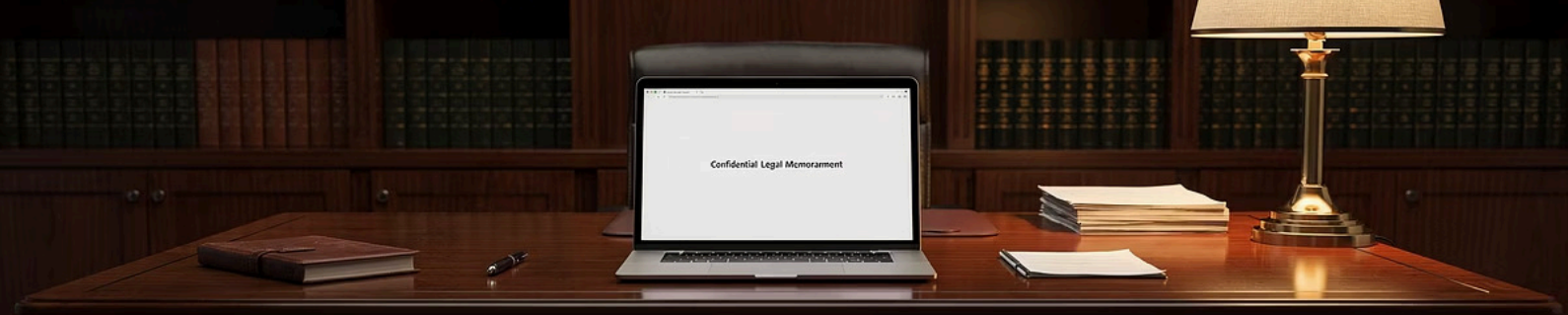
Cybersecurity e Modello 231 — strumento metodologico per aggiornare MOG e flussi verso l'OdV

#### **ESRS semplificati**

Riduzione *datapoint* obbligatori per la rendicontazione di sostenibilità

#### **Standard VSME**

Standard volontario per imprese non soggette agli obblighi CSRD — rilevante per PMI in *supply chain*



## VI. Giurisprudenza d'Impresa

### Cass. Pen. Sez. IV n. 16359 — 6 maggio 2026

DVR inadeguato: responsabilità penale del datore di lavoro e del RSPP

1

2

### Cass. Pen. n. 16218 — 5 maggio 2026

Cancellazione della società: estinzione dell'illecito 231

## Infortunio mortale e DVR inadeguato — Cass. Pen. Sez. IV n. 16359 del 6 maggio 2026

**Il Caso:** Infortunio mortale occorso durante la manutenzione di un autocarro il cui sistema di sicurezza era stato manomesso. Imputati il datore di lavoro e il RSPP.

**La Sentenza:** La Corte conferma la responsabilità: il **DVR** deve individuare non solo i pericoli tipici, ma anche quelli ragionevolmente prevedibili, incluse manomissioni e inefficienze dei dispositivi di sicurezza. Norme: **artt. 17, 28 e 29, D.Lgs. 81/2008**.

**Analisi Tecnica per il Board:** Il DVR va riletto come strumento dinamico. Auditare il processo di valutazione dei rischi sulle attrezzature e includere i rischi da manomissione e da comportamento scorretto ma non abnorme degli operatori.

## Cancellazione della società ed estinzione dell'illecito 231 — Cass. Pen. n. 16218 del 5 maggio 2026

**Il Caso:** Ente cancellato dal registro delle imprese in pendenza di un procedimento per illecito amministrativo dipendente da reato.

**La Sentenza:** La Corte afferma che la cancellazione dal registro delle imprese determina l'**estinzione dell'illecito 231**, in via analoga alla morte dell'imputato, risolvendo la questione sulla base dell'**art. 2495 c.c.** e rendendo inapplicabili le sanzioni del decreto.

**Analisi Tecnica per il Board:** Pronuncia di rilievo nelle operazioni straordinarie e nelle riorganizzazioni di gruppo; va però gestita con cautela, perché incide su confisca e profili di continuità d'impresa che richiedono valutazione legale specifica.



## VII. Azioni Prioritarie Consigliate — "Cosa deve fare il Board oggi"

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

1

### Aggiornare il Modello 231 sui reati ambientali

Avviare una *gap analysis* delle aree a rischio ambientale — gestione rifiuti, scarichi, emissioni, sostanze ozono-lesive e gas fluorurati — confrontando le fattispecie introdotte dal **D.Lgs. 81/2026** con i protocolli vigenti, per poi aggiornare la parte speciale del MOG e le procedure operative.

2

### Verificare lo stato NIS2 sul Portale ACN

Confermare che dati e figure responsabili sul Portale ACN siano stati aggiornati nei termini, completare la categorizzazione di attività e servizi tramite il nuovo *Servizio NIS/Categorizzazione* e verificare la corretta designazione del referente CSIRT. Previste sanzioni fino al **2% del fatturato annuo globale**.

3

### Censire i fornitori rilevanti (Det. ACN n. 127437/2026)

Individuare i fornitori critici per la continuità dei servizi, caricarne l'elenco nella piattaforma ACN e rivedere i contratti di fornitura inserendo clausole di sicurezza informatica e obblighi di notifica degli incidenti.

4

### Rivedere il DVR

Riesaminare il *Documento di Valutazione dei Rischi* includendo i pericoli da manomissione o malfunzionamento dei dispositivi di sicurezza, verificare l'adeguamento delle attrezzature agli standard e documentare con data la formazione del personale. Prevista la responsabilità penale di datore e RSPP per *colpa specifica*.

5

### Governare l'AI applicata al personale

Censire gli strumenti di IA già in uso o in valutazione sul personale e sottoporre ciascuno a una *DPIA* preventiva, verificandone la compatibilità con il divieto dell'**art. 5 AI Act** e con i limiti dell'**art. 4 dello Statuto dei lavoratori** prima di ogni adozione.

6

### Rafforzare le misure di sicurezza sui dati

Aggiornare e documentare l'analisi del rischio sui sistemi, definire un piano di risposta agli incidenti e pianificare test periodici di resilienza, dalle verifiche dei *backup* ai *penetration test*.



# BIELLE CONSULTING

Risk, Sustainability & Compliance

"Contattateci per ulteriori approfondimenti e per un assessment!"

## Sede

Via Thaon di Revel, 21 –  
20159 Milano

## Email

info@bielleconsulting.com

## Telefono

Simona Bellavia:  
+39 348 150 5622

Giacomo Leone:  
+39 346 087 5317

## Online

[linkedin.com/company/bielle-consulting](https://www.linkedin.com/company/bielle-consulting)

[www.bielleconsulting.com](http://www.bielleconsulting.com)