COMITATO COMPLIANCE 231 LEGALITA' Aicq – Associazione Italiana Cultura Qualità

Titolo Podcast n.3/2026:
PRIVACY BY DESIGN E BY DEFAULT: COME INTEGRARE LA PROTEZIONE DEI DATI NEI PROCESSI AZIENDALI

Podcast n.3/2026 COMITATO COMPLIANCE 231 LEGALITÀ AICQ

PRIVACY BY DESIGN E BY DEFAULT: COME INTEGRARE LA PROTEZIONE DEI DATI NEI PROCESSI AZIENDALI di Monica Palmisano, DPO e consulente in protezione dei dati personali

Benvenuti/e a questo nostro approfondimento.

Sulla base della sua esperienza, qual è l'equivoco più frequente che riscontra nelle organizzazioni quando si approcciano alla compliance e alla tutela della privacy?

L'equivoco più radicato è trattare la protezione dei dati come una checklist da spuntare a valle: a prodotto già sviluppato, processo già avviato, sistema già in produzione. È un approccio inefficiente e costoso: rimediare a posteriori significa riscrivere architetture, rinegoziare contratti, rivedere processi già operativi. I costi — economici, organizzativi, reputazionali — sono incomparabilmente maggiori rispetto a quelli di un'integrazione fin dall'inizio. E soprattutto si espone l'organizzazione a rischi concreti: data breach, sanzioni GDPR, responsabilità penali.

Se l'approccio 'a posteriori' è inefficace e rischioso, quale paradigma richiede la normativa per evitare di dover mettere le toppe a un sistema già avviato?

L'art. 25 del GDPR è molto chiaro: la tutela dei dati deve essere progettata dentro i sistemi fin dall'inizio, come la solidità di un edificio dipende dalle fondamenta e non dai lavori di rinforzo eseguiti dopo il collaudo. Questo è il nucleo della Privacy by Design e della Privacy by Default — due principi normativamente vincolanti. E non basta dichiararli: bisogna dimostrarli. Questo concetto si chiama accountability ed è uno dei pilastri del Regolamento. Questi principi vanno poi integrati con gli standard ISO — la 27001 sulla sicurezza delle informazioni e la 37301 sulla compliance — e con il Modello Organizzativo *ex* D.Lgs. 231/2001, formando un sistema coerente anziché silos separati.

Ha citato la Privacy by Design e la Privacy by Default, due concetti che oggi diamo per scontati ma che hanno radici ben precise. Da dove nascono esattamente e come si differenziano nella pratica aziendale di tutti i giorni?

La Privacy by Design nasce negli anni ‘90 con la giurista canadese Ann Cavoukian: la tutela della privacy non deve essere reattiva, un rimedio dopo il danno, ma incorporata nei sistemi fin dalla progettazione. Con il GDPR è diventato un obbligo dimostrabile: il titolare deve adottare misure tecniche e organizzative adeguate già al momento di determinare i mezzi del trattamento. La Privacy by Default impone invece che, per impostazione predefinita, siano trattati solo i dati strettamente necessari. Un esempio: i cookie banner conformi presentano i consensi facoltativi già deselezionati. Il Garante ha sanzionato più volte organizzazioni che avevano impostato le piattaforme con consensi pre-flaggati, violando esattamente questo principio.

Spesso vediamo la compliance privacy gestita come un 'silos' a sé stante. Come si inserisce la protezione dei dati nel quadro più ampio della governance e dei sistemi di gestione, come ad esempio le normative ISO?

La protezione dei dati è un sottoinsieme della sicurezza delle informazioni, con la specificità di tutelare anche i diritti fondamentali degli individui. La ISO/IEC 27001:2022 presidia riservatezza, integrità e disponibilità. Controlli dell'Annex A come la crittografia, la gestione degli accessi e la sicurezza nello sviluppo software attuano concretamente la Privacy by Design. La ISO/IEC 27701 — che estende la 27001 alla gestione della privacy — è il ponte normativo verso il GDPR e può dimostrare la conformità all'art. 25. La UNI ISO 37301:2021 aggiunge la dimensione della governance, richiedendo di integrare il GDPR nella cultura organizzativa. In

questo scenario Compliance Manager e DPO devono lavorare in sinergia, condividendo metodologia, mappatura degli obblighi e analisi del rischio.

Tra Regolamenti europei e Leggi nazionali, il rischio di creare sovrapposizioni è altissimo. Esiste un metodo operativo per unire i puntini ed evitare che questi sistemi di controllo si ignorino o si contraddicano?

È il punto più trascurato, eppure cruciale. Opera su due livelli.

Il primo: i reati presupposto. L'art. 24-bis del D.Lgs. 231/2001 include i principali delitti informatici — accesso abusivo a sistemi, intercettazione illecita di comunicazioni, danneggiamento di dati e sistemi. L'art. 167 del Codice Privacy sul trattamento illecito di dati personali, pur non essendo direttamente reato presupposto 231, assume rilevanza nella governance del rischio perché le condotte che integrano quella fattispecie spesso si intersecano con i reati informatici richiamati dall'art. 24-bis.

Il secondo livello riguarda i controlli preventivi: misure come pseudonimizzazione, cifratura, gestione dei log, separazione dei ruoli sono al tempo stesso protocolli di prevenzione 231 e misure di sicurezza *ex* art. 32 GDPR. Progettarle in modo integrato evita che i due sistemi si contraddicano.

L'approccio: tre cerchi sovrapposti — compliance normativa, sicurezza delle informazioni, protezione dei dati.

Molte organizzazioni sono già abituate a ragionare per processi o hanno già certificazioni. Come si può sfruttare questo linguaggio aziendale preesistente per 'mettere a terra' la Privacy by Design in modo continuativo e strutturato?

Sì, e il vantaggio è che non si tratta di reinventare la ruota. Il metodo è il ciclo PDCA — Plan, Do, Check, Act — linguaggio già comune a tutti i Sistemi di Gestione ISO. L'obiettivo è evitare di creare isole separate tra privacy, sicurezza e responsabilità dell'ente, costruendo un sistema integrato in cui ogni fase del ciclo produce valore per tutti e tre gli ambiti.

Partiamo allora dalla prima fase, il 'Plan'. All'atto pratico, da dove si inizia per mettere a terra questa convergenza senza raddoppiare o triplicare la burocrazia?

L'obiettivo è avere un'unica mappa dei processi aziendali, letta con lenti diverse: GDPR, sicurezza, D.Lgs. 231/2001. Il Registro dei trattamenti ex art. 30 GDPR va aggiornato partendo dalla stessa mappatura usata per il

Modello 231 e per il sistema UNI ISO 37301. Per ciascun processo si identificano: dati personali trattati, rischi per i diritti degli interessati, rischi di violazioni di legge, impatti sulla sicurezza. Il risultato è una valutazione del rischio integrata — non un documento solo privacy — che permette a DPO, CISO, Compliance Manager e Organismo di Vigilanza di parlare la stessa lingua.

Entrando nella fase di 'Do', ci può fare qualche esempio di come un singolo intervento possa risolvere contemporaneamente le esigenze di privacy, sicurezza informatica e Modello 231?

Bisogna progettare controlli multiscopo.

Tre esempi.

Primo: la minimizzazione dei dati — raccogliere solo ciò che è necessario riduce l'impatto dei data breach, limita il rischio di trattamento illecito ex art. 167 Codice Privacy e i danni da accesso abusivo rilevanti *ex* art. 24-bis D.Lgs. 231/2001.

Secondo: cifratura e pseudonimizzazione di database, backup e comunicazioni — attuano l'art. 32 GDPR, sono controlli dell'Annex A ISO 27001 e, nel Modello 231, dimostrano l'adozione di misure idonee a prevenire reati informatici.

Terzo: gestione degli accessi e segregazione dei ruoli — least privilege e log delle operazioni — riducono i trattamenti non autorizzati e producono evidenze per audit ISO, verifiche dell'OdV e controlli del Garante. Va affiancata una formazione mirata per chi progetta sistemi e procedure, perché la Privacy by Design entri davvero nelle specifiche di progetto.

Ha descritto una fase di verifica davvero rivoluzionaria: un unico cruscotto per la direzione aziendale. Cosa succede nell'ultima fase, per garantire che l'azienda impari dai propri errori?

Nella fase Check, invece di audit separati, si costruisce un unico programma di verifica che includa requisiti GDPR, controlli ISO/IEC 27001 e 27701 e protocolli 231. I data breach vengono analizzati con indicatori condivisi — numero, tipologia, tempi di rilevazione, cause — utili al DPO, all'OdV e alla funzione sicurezza. Le non conformità confluiscono nel registro UNI ISO 37301 e nel sistema disciplinare 231. Questo offre alla direzione una visione unitaria del rischio. La fase Act aggiorna l'intero sistema al cambiamento: nuove linee guida EDPB, provvedimenti del Garante, nuovi reati informatici, adozione di sistemi di IA. In questo contesto la DPIA *ex* art. 35 GDPR diventa lo strumento di raccordo tra i tre regimi: obbliga a mappare i

trattamenti, valutare i rischi e documentare le misure — un’analisi utile al DPO, all’OdV e al Compliance Manager.

Con l' IA - Intelligenza Artificiale che avanza rapidamente e il nuovo AI Act europeo, questo modello integrato è ancora sufficiente?

Privacy by Design e by Default non sono un onere: sono l'opportunità di costruire sistemi più robusti e affidabili, riducendo data breach, sanzioni GDPR ed esposizione ai reati informatici *ex* D.Lgs. 231/2001.

Ma con l’Intelligenza Artificiale che avanza a ritmi che la normativa fatica a seguire, mi chiedo se non sia già necessaria una vera e propria Ethics by Design, in cui la protezione dei dati sia solo uno dei valori fondamentali da incorporare nella progettazione.

L'AI Act europeo ci chiede già oggi di valutare rischi sistemici, bias algoritmici, trasparenza, supervisione umana. La DPIA diventa il raccordo naturale tra GDPR e AI Act. Rispondere a questa sfida sarà il lavoro dei prossimi anni.