UNIONE INDUSTRIALI
Torino

Convegno Associazione ICT Dott.Com 2026

Laura Marengo



Imprese: focus su trend GDPR e compliance

6 novembre 2026

Osservatorio Unione Industriali Torino

2.300 aziende associate

20 gruppi merceologici

Filiere:

DIGITAL INNOVATION
ENERGY AND SUSTAINABLE MOBILITY
ITALIAN LIFESTYLE
LIFE SCIENCES

PMI: 85% DELLE AZIENDE ASSOCIATE

TAVOLO PRIVACY E NUOVE TECNOLOGIE UNIONE INDUSTRIALI TORINO

GRUPPO DI LAVORO PRIVACY CONFINDUSTRIA

UNIONE INDUSTRIALI
Torino

La domanda centrale

- Non basta chiedersi: **“siamo conformi al GDPR?”**
- La domanda di **governance** è: **chi decide sull’uso del dato, con quali regole, con quali controlli e con quale prova?**
- Un dato attraversa funzioni, sistemi, fornitori, persone: il rischio nasce spesso nei passaggi di consegna , anelli deboli, …
- **Accountability** = capacità di dimostrare che scelte, misure e controlli sono adeguati al rischio e realmente attuati

ACCOUNTABILITY E GOVERNANCE

Dalla compliance documentale alla compliance dimostrabile:
non è più sufficiente avere informative, registro dei trattamenti e altri documenti GDPR, policy/procedure, … **MA**, occorre dimostrare che il rischio è presidiato, che i controlli, la formazione, la gestione degli incidenti e i flussi verso il DPO, funzionino effettivamente e vengano adeguatamente **GOVERNATI**

ACCOUNTABILITY: filo conduttore, metodo di **governance**. L'impresa deve essere in grado di dimostrare che il sistema funziona. L'imprenditore non è più davanti a un elenco di adempimenti da attuare ma è sempre di più al **centro della sua organizzazione** aziendale e deve lui stesso capire quali sono le misure adeguate alla sua realtà.
Questo richiede un diverso approccio e un cambiamento culturale che non tutte le piccole aziende sono già riuscite a fare

GOVERNANCE*:* **parola chiave, una governance efficace dei dati** non può essere considerata soltanto un adempimento normativo. **Deve diventare parte della gestione dell'innovazione e del patrimonio immateriale dell'impresa.** i **dati** stanno assumendo un valore sempre maggiore come vero e proprio **patrimonio competitivo dell'impresa**

Per il nostro sistema imprenditoriale questa è una sfida importante

Formazione: da obbligo a controllo

- **Formazione differenziata per ruolo**: CdA, management, IT/CISO, Risorse Umane, utenti, sviluppatori e utilizzatori di AI, …
- **NIS2** attribuisce rilievo alla formazione dei vertici aziendali e alla formazione dei dipendenti dei soggetti essenziali e important e indirettamente di quelli della loro filiera
- **AI Act**: alfabetizzazione in materia di IA per personale e soggetti che operano per provider/deployer e per gli utilizzatori
- **Misurare efficacia**: test, phishing simulation, errori ricorrenti, incidenti, richieste di support
- **Conservare evidenze**: programma, partecipazione, verifica, aggiornamenti

La supply chain è parte della governance

- **Responsabili del trattamento ex art. 28 GDPR e Terzi**

- **La Governance della filiera** costituisce una componente essenziale della **Data Governance**, in quanto assicura che i principi di protezione dei dati personali, sicurezza, accountability e conformità al GDPR siano applicati lungo l'intera catena del valore, includendo fornitori, partner e soggetti terzi coinvolti nel trattamento dei dati

- L'integrazione della gestione dei rischi di terze parti nei processi di **Data Governance** consente all'organizzazione di mantenere il controllo sui flussi informativi, presidiare i rischi derivanti dall'esternalizzazione e garantire un modello di responsabilità legalmente conforme

- **Ruolo fondamentale della filiera**: GDPR, NIS2, IA , Modelli Organizzativi 231, ESG,…

Team multidisciplinari

Vertici aziendali: strategia e governance; definizione degli indirizzi; approvazione delle politiche e allocazione delle risorse, …

Responsabile della protezione dei dati /DPO: GDPR e protezione dei dati; consulenza, sorveglianza della conformità privacy e valutazioni d'impatto, …

CISO / Responsabile sicurezza informazioni: Cybersecurity e NIS2; Gestione dei rischi informatici; sicurezza e resilienza, …

Responsabile IT: Sistemi informativi; Architetture tecnologiche; infrastrutture e integrazione dei sistemi, …

AI Officer / AI Governance Manager: Intelligenza artificiale e AI Act; Governance dei sistemi IA; classificazione dei rischi e supervisione del loro utilizzo; …

Legal e Compliance Officer: Diritto e regolamentazione; Interpretazione normativa; contratti e gestione della compliance; …

Risk Manager: gestione del rischio aziendale; Valutazione integrata dei rischi operativi, tecnologici e normativi; …

Responsabile Acquisti / Supply Chain: Gestione e valutazione dei fornitori; rischi di terze parti e clausole contrattuali; …

Risorse Umane / Formazione: Competenze e organizzazione; Formazione, sensibilizzazione e sviluppo delle competenze digitali; …

Responsabili delle funzioni aziendali; Processi e attività operative; Identificazione delle esigenze, dei rischi e degli impatti sui processi;

Internal Audit; Controlli indipendenti; Verifica dell'efficacia del sistema di governance e dei controlli; …

Focus sulla responsabilità degli amministratori

Artt. 2380-bis, 2381-bis e 2381-ter cod.civ.
La gestione e l'organizzazione dell'impresa spettano esclusivamente agli amministratori.
Valutazione dell'**adeguatezza dell'assetto organizzativo**, amministrativo e contabile della società sulla base delle informazioni ricevute.
Obbligo di agire informati.

Art. 2392, co. 1 cod.civ.
Gli amministratori devono adempiere i doveri ad essi imposti dalla legge e dallo statuto con la diligenza richiesta dalla natura dell'incarico e dalle loro specifiche competenze.

Nuovo ruolo del DPO

- NIS2, AI Act, DORA, Data Act e più in generale il nuovo corpus normativo digitale europeo stanno spostando il **DPO** da una funzione prevalentemente “privacy” a un nodo della **governance integrata** dei rischi digitali

- Questo non significa però che il DPO debba diventare CISO, AI Officer o responsabile della compliance NIS2: anzi, l'indipendenza richiesta dal GDPR impone di evitare sovrapposizioni che generino conflitti di interesse.

- **Come cambia il ruolo:** Tradizionalmente il perimetro del DPO era centrato su GDPR: informative, registri, DPIA, data breach, diritti degli interessati, rapporti con il Garante, privacy by design.

- Oggi un progetto digitale può contemporaneamente generare **rischio privacy, cyber, AI, lavoristico e di compliance**.

AI Act: è qui che il DPO cambia maggiormente

- Molte attività AI coinvolgono **dati personali**. In questi casi DPIA GDPR, valutazione dei rischi AI, data governance e — quando prevista — FRIA possono sovrapporsi significativamente.

- **NIS2: DPO e CISO devono lavorare molto più vicini**

- La **NIS2** porta la cybersecurity a livello di **governance aziendale** e responsabilità dell'organo di gestione. Per il **DPO** l'intersezione principale riguarda sicurezza dei dati personali, incidente informatico, fornitori, controllo degli accessi, …

- Un incidente cyber può infatti essere contemporaneamente un **incidente NIS2** e un **data breach GDPR**, con presupposti, destinatari e tempistiche di notifica differenti

- Il modello organizzativo dovrebbe quindi prevedere una procedura unica di **gestione degli incidenti**, dalla quale partano due valutazioni parallele: **Cyber incident → valutazione NIS2 + valutazione GDPR → notifiche appropriate.**
- Il DPO dovrebbe essere tempestivamente coinvolto nella seconda, senza diventare il responsabile operativo della cybersecurity

alcuni messaggi da considerare

- Il **dato** è un importante asset, ma anche fonte di vincoli e responsabilità
- Alla domanda posso fare un certo trattamento e/o utilizzare un nuovo Sistema di IA? La risposta non è NO ma è "**Si, ma valutando e governando i relative rischi"**
- Privacy, cybersecurity, contratti e AI richiedono una **governance integrata**
- La **supply chain** è parte del perimetro
- La **compliance** efficace produce evidenze
- La domanda che bisogna sempre farsi è: "**qual'è il punto debole della catena di governo del dato nella propria organizzazione"**

UNIONE INDUSTRIALI
Torino

Grazie,

Laura Marengo