Consulente - Formatore - Auditor

Mobile + 39 393.3265594 | **Sito** www.marcellocolaianni.it

Mail marcello@marcellocolaianni.it

Blog marcellocolaianniblog.wordpress.com

PRIVACY & AI GOVERNANCE

Percorso integrato

A CHI SI RIVOLGE

Pensato in particolare per organizzazioni che trattano dati personali in modo strutturato o che stanno introducendo strumenti di intelligenza artificiale nei propri processi, dalla PMI alla realtà più articolata, ovunque Privacy e AI richiedano un presidio coordinato.

DI COSA SI TRATTA

Un percorso integrato che unisce la protezione dei dati personali (GDPR e D.Lgs. 196/2003) alla governance dell'intelligenza artificiale (AI Act, Reg. UE 2024/1689). Tiene conto del *Digital Omnibus* europeo, che rinvia al 2027–2028 gli obblighi per i sistemi ad alto rischio, e della normativa italiana: la Legge 132/2025, il D.Lgs. 160/2026, che introduce il reato di omessa adozione di misure di sicurezza nei sistemi di IA e lo collega alla responsabilità degli enti ex D.Lgs. 231/2001, e il D.Lgs. 179/2026 su autorità e sanzioni.

GDPR e AI Act condividono oggetto ed esigenze: dati personali, decisioni automatizzate, valutazioni d'impatto, misure di sicurezza documentate. Per questo li affrontiamo insieme, con un sistema di gestione verificabile nel tempo basato su:

- **ISO/IEC 27001** e **27701**: sicurezza delle informazioni e gestione della privacy;
- **ISO/IEC 42001**: governance dell'IA in tutta l'organizzazione, per chi la sviluppa, la fornisce o la utilizza;
- **EN 18286**: il sistema qualità richiesto dall'art. 17 dell'AI Act ai fornitori di sistemi ad alto rischio, con presunzione di conformità in quanto citata nella Gazzetta Ufficiale dell'UE.

Integrate, ISO/IEC 42001 ed EN 18286 coprono sia la governance sia gli obblighi regolatori. Producono inoltre le evidenze (log, gestione dei rischi, documentazione tecnica, sorveglianza umana) anche per il modello 231.

Per la certificazione della conformità al GDPR è inoltre disponibile lo schema accreditato **ISDP 10003**.

PERCHÉ ADEGUARSI

RISCHIO - il mancato adeguamento al GDPR espone a sanzioni pecuniarie anche molto rilevanti e, nei casi più gravi, la normativa nazionale rimanda anche a responsabilità penali.
L'uso non governato di sistemi di intelligenza artificiale espone a rischi aggiuntivi, destinati a crescere quando

gli obblighi del *Digital Omnibus* diventeranno pienamente vincolanti.

VALORI - un presidio unico su Privacy e AI rafforza reputazione, affidabilità e credibilità dell'organizzazione nei confronti di clienti, partner e stakeholder, e dimostra un approccio proattivo alla trasformazione digitale, anziché rincorrere gli obblighi all'ultimo momento.

BISOGNO - le organizzazioni che trattano dati personali in modo strutturato, o che stanno introducendo strumenti di intelligenza artificiale nei propri processi, hanno bisogno di un presidio coordinato che copra entrambi gli ambiti con un solo referente e un solo ciclo di audit, anziché due consulenze scollegate.

SERVIZI EROGATI

- **Consulente Privacy / Privacy Manager:** in affiancamento all'organizzazione nell'adeguamento ed aggiornamento alla normativa al di fuori o internamente all'organigramma aziendale;
- **DPO (*Data Protection Officer* – Responsabile della protezione dei dati):** quale figura *super partes* di verifica e supporto all'Organizzazione e di riferimento nei confronti dell'Autorità garante e degli Interessati;
- **"Implementazione dei Sistemi di gestione: ISO/IEC 27001, 27701, ISDP10003** e **ISO/IEC 42001.** Schemi che concorrono alla conformità al GDPR (27001 e 27701 come presidio tecnico-organizzativo di supporto, ISDP10003 come schema di certificazione diretta del Regolamento) e all'AI Act (42001, framework di governance per i sistemi di intelligenza artificiale). Schemi di certificazione fra loro integrabili;
  - ↪ **Assistenza alla certificazione ISO/IEC 27001 - 27701 - 42001 e ISDP 10003:** supporto in sede di verifica ispettiva dell'Organismo di certificazione (Audit di 3^ parte)
  - ↪ **Assistenza**, relativa ai suddetti schemi, **in sede di qualificazione dei propri fornitori o da parte dei propri clienti** (Audit di 2^ parte)
  - ↪ **Assistenza**, relativa ai suddetti schemi, **in sede di verifiche ispettive interne** (Audit di 1^ parte)
  - ↪ Le suddette attività possono riferirsi ai singoli Sistemi di gestione oppure al Sistema di gestione integrato totale o parziale;
- **Audit privacy** - verifica dell'osservanza del GDPR e della sua applicazione da parte dei Responsabili del trattamento (art. 28)
- **Policy e governance AI** - regole interne per un uso conforme e consapevole di strumenti di intelligenza artificiale
- Valutazione d'impatto sui dati personali **(DPIA)** e sui diritti fondamentali per i sistemi ad alto rischio **(FRIA),** inclusa la classificazione del rischio degli strumenti in uso secondo l'AI Act;
- **Formazione integrata Privacy + AI** - percorsi per i diversi livelli e funzioni dell'organizzazione
- **Presidio di Governance & Organizzazione** - definizione di ruoli e responsabilità (titolare, DPO, referenti interni), leadership commitment richiesto dalle ISO, reporting verso il vertice sui rischi dati/AI.

IL MIO CONTRIBUTO

La materia richiede competenze multidisciplinari, non riconducibili a un unico profilo professionale: presidio GRC (governance, documentazione, sistemi di gestione), competenze tecniche specialistiche (validazione di modelli, conformity assessment dei sistemi ad alto rischio) e, competenze legali. Curo la componente GRC

in prima persona coinvolgendo le altre professionalità per quanto ai rispettivi punti specifici in cui la materia lo richiede.

APPROFONDIMENTI

Ampiezza ISO: *oltre a 27001 e 42001, restano disponibili su richiesta anche altri sistemi di gestione ISO (qualità, ambiente, sicurezza sul lavoro, energia, anticorruzione, compliance, ecc.), non promossi attivamente in questo pacchetto.*

Nota bene: il pacchetto è concepito in forma integrata per massimizzare le sinergie tra i servizi, ma ciascuna componente può essere richiesta anche singolarmente, in base alle esigenze specifiche del cliente.