

🎯 OBIETTIVI

Il GDPR ha obbligato le Pubbliche Amministrazioni ad un effettivo controllo sul trattamento dei dati in proprio possesso, ad una reingegnerizzazione di tutti i processi gestionali e all'introduzione di nuove misure tecniche di cyber security, nell'ambito delle politiche nazionali di sicurezza informatica.

Il corso è un valido strumento di compliance per la PA, analizzando le metodologie tecniche e gestionali e le misure organizzative e di cyber security che il DPO e gli altri soggetti devono mettere in pratica al fine di rispettare al contempo gli obblighi del GDPR e le prescrizioni in materia di trasparenza e accesso civico.

👤 DOCENTI

Gioele COLOMBI
Esperto di Cyber Security

Sergio CONTESSA
Esperto di ingegneria della PA e diritto nuove tecnologie

Michele MORRIELLO
Avvocato, Esperto di Digitalizzazione della PA

📍 LUOGO E DATA

FIRENZE, 20 e 21
maggio 2020

TUTELA DELLA PRIVACY E CYBER SECURITY NELLA PA DOPO IL GDPR: OBBLIGHI, COMPLIANCE, RESPONSABILITÀ

La compliance normativa e tecnica al GDPR. Le misure di sicurezza informatica dopo il D.L. 105/2019. I rapporti con trasparenza e accesso civico. Ruolo e funzioni del DPO e degli altri soggetti coinvolti

La tutela della privacy nella PA dopo il GDPR e il D.Lgs. 101/18. I principi guida. **Gli adempimenti obbligatori delle Pubbliche Amministrazioni:** la compliance normativa e tecnica al GDPR.

Le strategie di sicurezza informatica a livello nazionale.

La costituzione del **perimetro di sicurezza nazionale cibernetica** (D.L. 105/19 convertito in L. 133/19). Le **modalità attuative**.

La costituzione del **CSIRT** (DPCM dell'8/8/2019) e le funzioni di vigilanza sugli operatori dei servizi essenziali.

Analisi degli interventi del Garante della privacy e del Comitato europeo per la protezione dei dati: la valutazione d'impatto; la portabilità; i responsabili della protezione dei dati; le sanzioni amministrative pecuniarie; il *data breach*; l'informatica; il consenso; la trasparenza. Gli altri atti del Comitato.

I soggetti del sistema di gestione della privacy: il Responsabile, il *Data Protection Officer* e gli incaricati al trattamento. **Ruolo, funzioni e requisiti soggettivi del DPO.**

La nomina dei **responsabili esterni**. Le comunicazioni al Garante.

La gestione e l'aggiornamento del registro dei trattamenti. I contenuti obbligatori. **La mappatura delle attività svolte.**

Gli **obblighi di informativa** ed i **diritti dell'interessato**. I limiti al **"riutilizzo"**.

La **durata** degli obblighi di pubblicazione. Il **diritto all'oblio**.

Il rapporto tra GDPR e obblighi di trasparenza e accesso civico generalizzato delle Pubbliche Amministrazioni.

I rapporti tra **DPO e RPCT**.

La sicurezza informatica nel settore pubblico: stato dell'arte e scenari futuri. **Le misure tecniche di cyber security.** *Best practices*. L'impatto sulle procedure interne delle Pubbliche Amministrazioni.

Le **misure minime di sicurezza obbligatorie** (Circolare AGID 2/2017) e le sfide della PA sul *data protection*. La valutazione dei rischi sulla protezione dei dati tra **policy di sicurezza e cyber crimine**. Monitoraggio e **log management**.

Le modalità di conservazione e cancellazione sicura dei dati personali.

Gli adempimenti e le responsabilità delle figure che operano in qualità di **amministratori di sistema**.

La privacy e l'utilizzo del cloud. Le nuove disposizioni in materia di **reti 5G** (D.L. 105/19). Le applicazioni della **blockchain per la PA**.

I Regolamenti del Garante della Privacy 1/2019 e 2/2019 su tempi e procedure interne del Garante in materia di provvedimenti correttivi e sanzionatori. Gli obblighi di segnalazione alla Magistratura competente.

Le nuove ipotesi di responsabilità previste dal GDPR. L'inasprimento del sistema sanzionatorio.

Le **responsabilità civili** delle Amministrazioni e degli operatori. Il rischio risarcitorio e il problema dell'individuazione dei danni materiali e immateriali.

Le **responsabilità penali**. Le fattispecie di reato dopo il D.Lgs. 101/18.