

LA GESTIONE DELLA PRIVACY NELLA PA DOPO GDPR E D.LGS. 101/18: OBBLIGHI, CYBER SECURITY, RESPONSABILITÀ

Gli interventi del Garante della Privacy. Il registro dei trattamenti. Le misure di sicurezza informatica. I rapporti con trasparenza e accesso civico. Il ruolo e le responsabilità dei soggetti coinvolti

La tutela della privacy nella PA dopo il GDPR e il D.Lgs. 101/18 di coordinamento con la normativa nazionale.

I principi guida del GDPR. La privacy by design e by default. La responsabilizzazione dei soggetti (accountability).

Analisi degli ultimi interventi del Garante per la protezione dei dati personali. L'aggiornamento delle autorizzazioni generali.

Il ruolo del Comitato europeo per la protezione dei dati e le Linee guida del Gruppo di lavoro art. 29: la valutazione d'impatto sulla protezione dei dati; la portabilità dei dati; i responsabili della protezione dei dati; le sanzioni amministrative pecuniarie; il data breach; l'informativa; il consenso; la trasparenza.

Il Responsabile della privacy e gli incaricati al trattamento.

Ruolo, funzioni e requisiti soggettivi del Data Protection Officer (DPO). La banca dati dei DPO presso il Garante della Privacy.

La valutazione dei **oggetti che concorrono con la PA al trattamento dei dati personali** e la nomina dei **Responsabili esterni**.

I rapporti tra DPO e RPCT (PNA 2018).

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

L'individuazione di **specifiche tecniche di tutela della sicurezza**.

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

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

Le nuove misure di cyber security.

Le **misure minime di sicurezza obbligatorie** e le sfide della PA sul data protection (Circolare AGID 2/2017). I rischi interni ed esterni sulla protezione dei dati tra **policy di sicurezza e cyber crimine**.

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 applicazioni della **blockchain per la Pubblica Amministrazione**: le nuove possibilità in termini di cyber security.

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

I limiti generali alla trasparenza. Le Linee guida e i pareri del Garante della Privacy. Le Linee guida ANAC.

I limiti e le modalità di pubblicazione dei dati personali e il divieto di pubblicazione di dati ulteriori rispetto alle finalità di trasparenza.

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

Le **responsabilità civili** delle Amministrazioni e il problema dell'individuazione dei danni materiali e immateriali.

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

📌 OBIETTIVI

Il GDPR, General Data Protection Regulation, e il D.Lgs. 101/2018 di coordinamento obbligano ormai le Pubbliche Amministrazioni ad un effettivo controllo sul trattamento dei dati in proprio possesso e ad una reingegnerizzazione di tutti i processi gestionali, applicando nuove misure di sicurezza informatica.

Il corso analizza le metodologie tecniche e gestionali e le misure di cyber security che il DPO e gli altri soggetti responsabili devono mettere in pratica al fine di rispettare al contempo i nuovi obblighi del GDPR e le prescrizioni in materia di trasparenza e accesso civico.

👤 DOCENTI

Sergio CONTESSA

Esperto di ingegneria della PA e diritto nuove tecnologie

Michele MORRIELLO

Avvocato, Esperto di Digitalizzazione della PA

Valerio SARCONI

Presidenza del Consiglio dei Ministri

📍 LUOGO E DATA

ROMA, 13 e 14 febbraio 2019