



## Gli Amministratore di Sistema alla luce del GDPR AdS secondo la direttiva UE 679/2016

### Descrizione

Il 4 Maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il "Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

Il Regolamento entrerà in vigore il 25 Maggio 2016 e sarà concretamente operativo nei Paesi UE a decorrere dal 25 maggio 2018, lasciando a tutti i soggetti interessati un biennio di tempo per gli adeguamenti necessari alle proprie politiche del trattamento dei dati.

Per quanto riguarda l'Italia, il Regolamento sostituirà il "Codice Privacy" in vigore dal 1° Gennaio 2004.

L'amministratore di sistema, pur non essendo esplicitamente richiamato nel GDPR, ha una considerevole responsabilità sui dati aziendali e riveste un ruolo particolare sul piano operativo all'interno dell'azienda. Quali sono le prerogative e le funzioni di questa figura e gli obblighi previsti dal Garante Privacy

L'amministratore di sistema o, tecnico sistemista di rete, è una figura professionale che approfondisce le competenze di un tecnico hardware e software soprattutto per quanto riguarda le caratteristiche delle architetture informatiche e, in particolare, l'utilizzo e la condivisione di grandi quantità di dati attraverso le reti di comunicazione.

**Durata: 3 giorni**

Si occupa quindi essenzialmente di ogni tipo di rete informatica, comprese quelle a cui non si accede via web, come le reti intranet e implementa i sistemi di sicurezza del networking nonché definisce le procedure di autenticazione alla rete e di autorizzazione all'accesso ai dati da parte gli utenti, curando interventi di conservazione dei dati attraverso debite soluzioni di "backup" e progettando le attività di supporto al "disaster recovery".

### A chi si rivolge

- Responsabile IT, Security Manager, Compliance Officer;
- liberi professionisti che svolgano attività di consulenza

### I principali Argomenti trattati

- L'amministratore di sistema nel GDPR
- Chi è l'amministratore di sistema
- La valutazione d'impatto sulla protezione dei dati
- Le funzioni dell'amministratore di sistema
- La normativa ed i provvedimenti del Garante
- Gli obblighi previsti dal Garante Privacy
- I risvolti "lavoristici" della designazione degli amministratori di sistema

## Contenuti

### Modulo 1: Il Regolamento Europeo UE679-2016

- Il nuovo Regolamento UE 2016/679
- Trattamento e tipologia di dati
- I diritti dell'interessato, informativa e consenso
- Gestione informative, consensi e richieste agli interessati (artt. 13 e 14 GDPR)
- Registro dei trattamenti (art.30 GDPR)
- Come redigere un'informativa per un sito web
- Organigramma Privacy nelle aziende, Ruoli e Responsabilità
- Come nominare un responsabile ed individuare un incaricato del trattamento
- Analisi dei rischi
- Sistema di Gestione della Sicurezza delle Informazioni (ISMS)
- Misure di Sicurezza, minime e idonee
- Notificazione del trattamento al Garante
- Il Garante della Privacy: compiti e funzioni
- Sanzioni, violazioni amministrative e penali, risarcimento del danno
- La Videosorveglianza
- Come predisporre una Notifica all'Autorità Garante ai sensi dell'art. 37 TU Privacy
- Il Data Protection Officer o Responsabile della Protezione dei dati personali art. 37 GDPR, cenni

### Modulo 2: La figura dell'amministratore di sistema

- Misure idonee e misure minime
- Misure per il trattamento informatico
- L'inventario dei trattamenti
- La valutazione di impatto privacy
- La violazione di dati personal
- Cookie e Privacy: istruzioni per l'uso
- WP 29 e linee guida sulle app
- Policy e Privacy sul lavoro (uso della posta elettronica aziendale ed internet)
- La videosorveglianza in Azienda
- Gestione di sistemi di autenticazione, profilazione ed autorizzazione
- Custodia delle credenziali
- Gestione dei flussi di rete
- Gestione del back-up e sistemi di Recovery

### Modulo 3: Registrazione degli accessi degli ADS

- Identificazione e tracciamento degli accessi logici
- Modalità e tempi di conservazione
- Misure di sicurezza
- Responsabilità nella conservazione
- Comunicazione e informativa agli utenti
- Amministratori di Sistema e Log
- Cookie e Privacy: istruzioni per l'uso
- WP 29 e linee guida sulle app
- Policy e Privacy sul lavoro (uso della posta elettronica aziendale ed internet)
- la gestione degli elenchi degli ADS
- controlli sugli accessi ai sistemi
- verifiche sull'operato degli amministratori

### Modulo 4: Nuovi compiti per l'ADS

- Linee guida WP29 sulla Portabilità del Dato
- Linee guida WP29 sulla Valutazione di impatto privacy
- Reati informatici e cybercrime
- Individuazione del ruolo privacy del fornitore
- Regole per la sicurezza dei dati in rete e nelle telecomunicazioni

### Modulo 5: Privacy e Cloud Computing

- Cos'è il Cloud Computing
- I principali servizi del Cloud e la definizione del NIST (IaaS, PaaS, SaaS).
- Il Cloud Computing: profili privacy
- Definizione di "rischio" e sicurezza per la migrazione al Cloud.
- Requisiti di sicurezza del Cloud Computing

### Modulo 6: Modulistica

- Registro Elenco AdS
- Procedura - Gestione Violazioni Dati Data Breach
- Scheda segnalazione incidente
- Procedure di Audit Interno