

“II DATA PROTECTION OFFICER”

Titolo	DATA PROTECTION OFFICER
Destinatari	Il consulente esterno della Privacy deve essere designato sulla base della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati
Obiettivi e finalità	<ul style="list-style-type: none"> - A dotarsi in organico di un Data protection officer, devono essere tutte le imprese pubbliche e private che svolgono trattamenti (sui dati) potenzialmente in grado di ledere gravemente i diritti degli interessati e hanno, pertanto, la necessità di essere monitorati da un soggetto che sia indipendente rispetto alle logiche aziendali.
Normativa di riferimento	<ul style="list-style-type: none"> - Regolamento Europeo Privacy 2016/79;
Requisiti di ammissione	Conoscenza di base della Normativa Privacy. Conoscenza generale della terminologia italiana e anglosassone correntemente usata in ambito sicurezza informatica.
Durata e modalità	Il corso ha una durata di 80 ore erogate completamente in modalità e-learning (L.M.S.) Learning Management System, in grado di monitorare e di certificare lo svolgimento, la tracciabilità e il completamento delle attività didattiche di ciascun utente.
Programma del corso	DISCIPLINE E CONTENUTI
	<p>MODULO 1 – La protezione dei dati personali</p> <ul style="list-style-type: none"> - Privacy by design e by default: fin dalla progettazione e per impostazione predefinita - Database e applicativi utilizzati - Sistemi distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets (es. big data) - Attacco informatico e contromisure per evitarli - Analisi criminologica di sistemi informativi - Tecniche crittografiche, di anonimizzazione e di pseudonimizzazione

	<p>MODULO 2 – Rischi Plausibili</p> <ul style="list-style-type: none"> - Gestione del Marketing in e out - Web Marketing - Le minacce cyber - Sistemi e tecniche di monitoraggio e "reporting"- - Le possibili minacce alla protezione dei dati personali - Le trappole cognitive nel processo di valutazione del rischio - Valutazione delle probabilità di accadimento di un rischio <p>MODULO 3 – Conformità del trattamento</p> <ul style="list-style-type: none"> - Verifica della conformità del trattamento alle prescrizioni del Regolamento - - Adesione ai codici di condotta - Le best practice (metodologie) e gli standard nella analisi del rischio e nella gestione della sicurezza delle informazioni - Il potenziale e le opportunità offerte dagli standard e dalle best practices più rilevanti - Le nuove tecnologie emergenti (es. sistemi distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets) <p>MODULO 4 – Investimenti e Sanzioni</p> <ul style="list-style-type: none"> - Data Breach: la notifica della violazione dei dati all’Autorità di controllo e all’interessato - Il Trattamento Dati nella SSL e nella “231” – Responsabilità Amministrativa dell’Ente - Whistleblowing - Il sistema sanzionatorio relativo alle violazioni concernenti dati e informazioni di tutti i tipi - Le sanzioni stabilite dalla normativa Privacy comminate dal GDPR - il ritorno dell’investimento connesso all’abbattimento del rischio ed il valore aggiunto per l’Ente - Esercitazione <p>MODULO 5 – Competenze del DPO</p> <ul style="list-style-type: none"> - I metodi di sviluppo delle competenze - i tipici KPI (key performance indicators) - Le metodologie di analisi dei fabbisogni di competenze e skill - La Linea guida sui responsabili della protezione dei dati (RPD) e la norma UNI 11679 - Conoscenze, abilità e competenze tipiche del DPO
<p>Valutazione</p>	<p>La valutazione finale verrà effettuata mediante una verifica di apprendimento finale (esame finale).</p>
<p>Attestato formativo rilasciato</p>	<p>Attestato di frequenza del corso di “Data Protection Officer” rilasciato dall’A.I.S.F.</p>