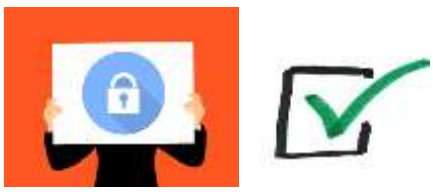
DPCORE.EU

ASSO DPO
Associazione Data Protection Officer
Associato

LA NUOVA PRIVACY AZIENDALE EUROPEA

Il 25 maggio 2018 entrerà in applicazione il **nuovo Regolamento Generale sulla Protezione dei Dati Personali GDPR - UE 2016/679,** già approvato durante il 2016. Non sono previsti né ritardi, né rinvii.

Tutte le aziende con sede nell'Unione Europea, o al di fuori, **che raccolgono o elaborano dati personali e particolari** (sensibili) di cittadini dell'UE, **dovranno implementare nei propri processi vari adeguamenti sia tecnologici che organizzativi per essere conformi a tale Regolamento**.

QUALI SONO I DATI A CUI SI RIFERISCE IL REGOLAMENTO EU GDPR - 2016/679 SULLA PRIVACY?	• Dati personali e particolari (sensibili) • Identificativi on-line, login e password, cookies, indirizzi IP, ubicazione GPS, ecc. • Dati genetici • Dati biometrici • Dati relativi allo stato di salute • Dati relativi a situazioni giudiziarie	
A CHI INTERESSA L'ADEGUAMENTO AL REGOLAMENTO EU GDPR - 2016/679?	• Fornitori di servizi che processano dati personali o particolari (sensibili) • Servizi Cloud • Call center • Aree amministrative / contabili • Medici, laboratori di analisi e cliniche mediche • Avvocati • Professionisti e aziende in generale che trattano dati particolari (sensibili)	
QUALI SONO GLI OBBLIGHI PER LE AZIENDE?	• **Privacy by design**: Incorporare i fondamenti della privacy a partire dalla progettazione di qualsiasi processo aziendale per garantire la protezione dei dati personali e prevenire i rischi • Istituzione di un **Registro per il trattamento dati** ed assunzione di responsabilità • Nomina di **Titolare e Responsabile del trattamento dati** • **Valutazione dei rischi** e dell'impatto sulla protezione dei dati • **Notificare al Garante della Privacy** un'eventuale violazione dei dati personali • Procedure standardizzate per il **trasferimento dati**	
COSA DEVONO GARANTIRE LE AZIENDE AGLI UTENTI PER I QUALI TRATTANO I DATI?	• Acquisizione del **consenso al trattamento dati** • **Diritto di rettifica, aggiornamento e cancellazione** dei dati personali • **Portabilità dei dati** da un fornitore di servizi all'altro • Diritto di non essere sottoposti ad un **trattamento automatizzato dei dati**	
COSA CAMBIA PER LA SICUREZZA E LE MODALITA' DI TRATTAMENTO DEI DATI?	• Applicare misure tecniche ed organizzative per garantire **un livello adeguato di sicurezza dei dati** • Il Titolare del trattamento **deve conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità** • **Occorre dimostrare la concreta adozione delle misure tecniche ed organizzative**	
COSA SI RISCHIA IN CASO DI INADEMPIMENTO AL GDPR UE 2016/679?	• **Sanzioni pecuniarie** fino a **€ 20 milioni** o **4% del fatturato** mondiale annuo • **Richieste di risarcimento** per eventuali danni causati agli interessati • **Screditamento dell'immagine** aziendale e **perdita di fiducia** dei consumatori	

Per info: Mob. +39 334.70.88.422 / fax: +39 941.931.11/ francesco.speciale@dpcore.eu / www.dpcore.eu

DPCORE.EU

ASSO DPO Associazione Data Protection Officer Associato

COSA OCCORRE FARE NEL CONCRETO?

Aspetto Tecnologico	Aspetto Normativo	Aspetto Organizattivo
Censimento Asset	Conoscere GDPR altre leggi Privacy	Organigramma Privacy
Data Discovery	Inventory Ruoli e proced. processi	Formalizzazione Ruoli Privacy
Analisi di Vulnerabilità	Formalizzazione Ruoli Privacy	Audit del Flusso dei dati personali
Protezione dei Dati Personali	Gestione Registro dei Trattamenti	Trasferimento dati verso l'estero
Minizzazione dei rischi	Procedure DPIA / Prior Check	Relazioni con Garante Privacy
Ottimizzazione Backup e DR	Reporting e Workflow	Corsi di Formazione

Registro dei Trattamenti	Il Titolare ed il Responsabile devono tenere un **Registro di tutte le attività di trattamento svolte sotto la propria responsabilità**. Il Registro consentirà di riscontare il percorso di compliance dell'organizzazione con il GDPR.
DPIA (Data Protection Impact Assessment)	La **Valutazione d'impatto sulla protezione dei dati** (DPIA in inglese) è una procedura obbligatoria per i Titolari qualora un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate.
DPO (Data Protection Officer) o Responsabile della Protezione dei dati	Il **Responsabile della Protezione dei dati** è una figura che dovrà sorvegliare l'osservanza del Regolamento EU, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità.
Gestione delle vulnerabilità (Vulnerability Management)	Ogni organizzazione deve eseguire periodicamente un'analisi di Vulnerability Management al fine di **essere pienamente informato e consapevole delle priorità dei rischi** della sua organizzazione.
Violazione dei dati personali (Data Breach)	In caso di Data Breach il **Titolare deve comunicare entro 72 ore al Garante della Privacy la natura della violazione dei dati personali**, le categorie e il n. approssimativo di interessati, le possibili conseguenze e le misure adottate.

Il rispetto del Regolamento europeo GDPR 2016/679 può avvenire solo attraverso un **percorso che si articola in una serie di tappe e di traguardi intermedi** (ad es. la richiesta di consenso, procedure per il rispetto dei diritti degli interessati, il coinvolgimento del DPO in ogni nuova campagna marketing o nuovo servizio). Grazie a questo percorso, la nuova Privacy Europea non dovrà essere più vissuta più come un obbligo di legge da adempiere, ma come un **momento d'innovazione organizzativa e tecnologica che potrà consentire di creare un nuovo rapporto di fiducia e di rispetto con i propri clienti, i propri partner e le Autorità.**

Per info: Mob. +39 334.70.88.422 / fax: +39 941.931.11/ francesco.speciale@dpcore.eu / www.dpcore.eu