REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
REGOLAMENTO (UE) 2016/679

Il nuovo Regolamento europeo sulla protezione dei dati personali (Regolamento (UE) 2016/679) è stato approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione il 4 maggio 2016.
La sua entrata in vigore è il 24 maggio 2016. Entro due anni a partire da tale data, ***(25 maggio 2018)*** tutti gli Stati membri dell'Unione devono uniformare la propria legislazione alle nuove regole comunitarie.
Il GDPR sostituirà quindi a tutti gli effetti il Decreto Legislativo del 30 giugno 2003 n. 196 «Codice in materia di protezione dei dati personali» e imporrà alle Organizzazioni destinatarie una serie di adeguamenti che dovranno essere pianificati per tempo con particolare riferimento ai seguenti aspetti:

- ✓ ***PRINCIPI PER IL TRATTAMENTO LECITO DEI DATI PERSONALI, TRA CUI GESTIONE DELL'INFORMATIVA E DEL CONSENSO***

  Al fine di rendere più semplice la lettura dell'informativa da consegnare all'interessato del trattamento, è previsto il ricorso ad icone esplicative e l'uso di un linguaggio semplice e chiaro.

  Il consenso deve essere libero, specifico, informato ed è valido se la volontà espressa non è equivoca. Nel caso di informativa digitale sui siti, non è obbligatorio il segno di spunta ma basta un testo che informa che proseguendo si accetta il trattamento dei dati con un link all'informativa.

- ✓ ***GESTIONE DELLE RICHIESTE E DEI DIRITTI DEGLI INTERESSATI AL TRATTAMENTO DEI DATI PERSONALI***

  Una novità importante è il principio di portabilità dei dati, nei casi in cui si ha la necessità di trasferire i propri dati da un gestore ad un altro e che dovrà essere reso più agevole da parte delle aziende.

  DIRITTO ALL'OBLIO Scatta anche il diritto all'oblio, cioè la facoltà dell'interessato a veder cancellati parte dei propri dati presenti in Rete, salvaguardando comunque il diritto di cronaca per i casi di rilevante interesse generale o per finalità di interesse storico.

- ✓ ***ORGANIZZAZIONE, RUOLI E RESPONSABILITÀ E NOMINE PER IL TRATTAMENTO DEI DATI PERSONALI: TITOLARE, RESPONSABILE E LA NUOVA FIGURA DAL "DATA PROTECTION OFFICER" (DPO);***

  Per supportare il Data Controller (titolare del trattamento) in questa delicata fase è stata istituita la figura del **Data Protection Officer** il quale dovrà effettuare il cosiddetto **Privacy Impact Assessment** (in pratica, la valutazione del rischio già presente nel **vecchio** decreto 196/2003) al fine di valutare le misure e gli accorgimenti da suggerire alle aziende per rispettare le norme del Regolamento, con la produzione della relativa documentazione sulle misure adottate per la tutela i dati. Tale valutazione sarà obbligatoria per le pmi in presenza di un rischio elevato.

  La nomina del Data Protection Officer è obbligatoria per le Pubbliche Amministrazioni e per le aziende che trattano particolari tipologie di dati sensibili o che effettuano la profilazione degli utenti. Ma, essendo le sanzioni non trascurabili, è bene valutare attentamente il ricorso a tale figura anche per le aziende che non rientrano strettamente in questi casi.

- ✓ ***MAPPATURA DEI TRATTAMENTI EFFETTUATI E RELATIVO REGISTRO DEI TRATTAMENTI;***

  L'articolo 30 impone al Data Controller (il titolare del trattamento) la redazione e l'aggiornamento del Registro delle attività del trattamento, ove sono descritti i trattamenti effettuati e le procedure di sicurezza adottate. Una cosa molto simile ad Documento Programmatico della Sicurezza della legge 196/2003 ma molto più rigoroso, soprattutto per i soggetti che trattano dati sensibili o giudiziari.

- ✓ ***GESTIONE DEI RISCHI PER IL TRATTAMENTO E ADOZIONE DELLE MISURE TECNICHE ORGANIZZATIVE PER IL TRATTAMENTO DEI RISCHI, NEL RISPETTO DEI PRINCIPI DELLA "PRIVACY BY DESIGN" E "PRIVACY BY DEFAULT" E PER IL PERSEGUIMENTO DI OBIETTIVI DI SICUREZZA DELLE INFORMAZIONI (DISPONIBILITÀ, INTEGRITÀ E RISERVATEZZA) E DI RESILIENZA;***

  Il nuovo Regolamento Europeo ha posto notevole attenzione alla responsabilità nei confronti degli utenti introducendo il principio della **privacy by design**, cioè l'obbligo di pianificare fin dall'inizio del processo produttivo (sia di un software che di un prodotto) un'attenta analisi dei rischi, la cosiddetta **Privacy Assessment**, al fine di assicurare la correttezza, l'integrità, a riservatezza e la sicurezza dei dati, nonché la effettiva cancellazione quando richiesta.

  Il principio della **privacy by default**, inoltre, mette in rilievo la condizione che gli strumenti e le modalità del trattamento devono essere contenute nei limiti del trattamento minimo necessario per il perseguimento del fine per cui tali dati vengono raccolti.

- ✓ ***VALUTAZIONE PREVENTIVA DI IMPATTO SULLA PROTEZIONE DEI DATI TRATTATI RISPETTO ALLE LIBERTÀ E AI DIRITTI DEGLI INTERESSATI;***

  In quest'ottica si pone anche il principio di **accountability**, cioè l'obbligo, da parte delle Pubbliche Amministrazioni e dei privati che trattano dati personali, non solo di rispettare formalmente le norme del Regolamento ma anche di mettere in pratica quanto stabilito in fase

di analisi dei rischi. Cioè, in caso di controversie, i titolari del trattamento dovranno dimostrare di aver attuato tutte le norme previste per ridurre al minimo i rischi di perdita dei dati o loro violazione, mettendo a punto le procedure necessarie alla risoluzione dei problemi e attuando criteri di trasparenza nei confronti dei soggetti a cui si riferiscono le informazioni.

- ✓ ***GESTIONE DEGLI INCIDENTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E NOTIFICA ALL'AUTORITÀ GARANTE.***

  È stato introdotto il cosiddetto principio di **Data Breach**, che scatta in caso di violazione dei dati, accesso abusivo o, comunque, perdita degli stessi: i titolari dei trattamenti saranno obbligati ad avvisare l'Autorità di Controllo e, nei casi di particolare gravità, anche i diretti interessati entro 72 ore

- ✓ ***FORMAZIONE E SENSIBILIZZAZIONE PER LE FIGURE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI;***

In definitiva, il nuovo Regolamento pone al centro del trattamento la tutela dei dati dell'interessato, tenendo conto sia dell'evoluzione delle tecnologie a disposizione per la protezione dei dati raccolti, sia della globalizzazione che ha ampliato enormemente la platea degli attori coinvolti nei processi di raccolta e diffusione dei dati.