

ADEGUAMENTO DEGLI STUDI PROFESSIONALI AL REGOLAMENTO UE/679/2016 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: I DOCUMENTI E I MODELLI DEL CNF

Carissimi Colleghi, come molti di Voi già sapranno, il 24 maggio 2016, vent'anni dopo l'introduzione in Italia della prima Legge organica sulla protezione dei dati personali (Legge n. 675/1996), sostituita nel 2003 dal c.d. Codice Privacy, è entrato in vigore il Regolamento UE 2016/679 (General Data Protection Regulation – GDPR).

Il Regolamento abroga la Direttiva 95/46/CE, innestandosi nel corpus normativo vigente senza comprometterne la validità e l'efficacia: i principi, gli obiettivi e gli istituti cristallizzati nel Codice Privacy, dunque, conserveranno validità ed efficacia anche quando, dal 25 maggio 2018, il GDPR diventerà direttamente applicabile in tutti i Paesi UE.

Nondimeno, la complessità e la portata innovativa del sistema regolamentare europeo impone all'interprete un'analisi al contempo dettagliata e coordinata con la disciplina nazionale, e ai Titolari del trattamento – in particolare professionisti, imprese e pubbliche amministrazioni – una ristrutturazione sistematica e multisettoriale del proprio assetto organizzativo, informata ai principi portanti della privacy by design e della privacy by default.

È precisamente questa la ragione del differimento applicativo previsto dal Legislatore europeo: i soggetti – pubblici e privati, individuali e collettivi, imprenditoriali e professionali – che svolgono attività di trattamento di dati personali hanno a disposizione un “periodo di adattamento”, fino al 25 maggio 2018, data in cui le nuove regole avranno applicazione diretta e cogente nel nostro ordinamento (così come in tutti gli ordinamenti nazionali degli Stati membri).

Il trattamento del dato personale, nella ratio del legislatore europeo, si sposta in modo evidente verso una corretta procedura di protezione dei dati personali trattati e detenuti dai soggetti (Titolari e Responsabili del trattamento dei dati personali) indicati dall'art. 4, nn°7 e 8 del Regolamento UE 2016/679.

Nell'ottica del principio di Accountability, sancito nelle disposizioni del GDPR, qualsiasi organizzazione - compresi i nostri Studi professionali - dunque, dovrà necessariamente procedere con una approfondita auto-analisi in merito sia alla circolazione (interna ed esterna) dei propri dati personali e quindi alle procedure in essere per legittimarne il trattamento, e sia alle misure di protezione in relazione ai dati personali detenuti. Inoltre, si dovrà tenere monitorata la correttezza delle procedure di trattamento e protezione dei dati personali soprattutto sotto il profilo giuridico, oltre che sotto il profilo tecnico-informatico.

Si precisa in proposito che non va assolutamente confuso il modello organizzativo di assessment per la protezione del dato - che va finalizzato attraverso una metodologia di analisi prevalentemente organizzativa e di controllo – con il solo sviluppo di politiche di sicurezza informatica a protezione del patrimonio informativo e documentale, le quali per poter essere utili ai fini del GDPR vanno soppesate in base all'analisi preventiva indispensabile in ragione alla tipologia dei dati trattati e ai rischi reali che corrono i propri database e archivi.

In particolare per essere “compliant” rispetto alle norme del GDPR, non sarà più sufficiente adottare un approccio meramente formalistico che si traduceva sino a oggi, nella maggior parte dei casi, nell'adozione delle misure minime di sicurezza di cui all'Allegato B del D.Lgs. 196/2003, nella redazione di informative e nomine a responsabili e incaricati e nell'acquisizione dei consensi degli interessati, ove necessario. Nel nuovo scenario normativo infatti, che delinea un approccio di Accountability (ovvero di “responsabilizzazione”), il Titolare del trattamento deve porre in essere tutte le misure di sicurezza in termini sì tecnologici, ma soprattutto organizzativi, adeguate a dimostrare (e documentare) di aver improntato i trattamenti di dati personali ai principi della Privacy by design e alla Privacy by default (a mero titolo esemplificativo: istituendo e alimentando correttamente il Registro dei trattamenti; adottando una procedura per analizzare i rischi di ogni

trattamento e quindi decidere se effettuare un Privacy Impact Assessment; verificando che l'archiviazione dei dati personali nelle banche dati dei nostri Studi professionali sia strutturata in modo idoneo e permetta anche di poter garantire agli interessati i nuovi diritti riconosciuti agli stessi dal GDPR, etc.).

Al fine di fornire delle prime indicazioni operative, dunque, segnalo la pubblicazione sul sito del Consiglio Nazionale Forense di alcuni documenti utili (reperibili al link: <http://www.consiglionazionaleforense.it/web/cnf/-/gdpr-linee-guida-avvocati>), tra cui una guida intitolata "Il GDPR e l'Avvocato", un Modello di informativa e uno Schema di registro delle attività di trattamento.

Cordiali saluti

Il Data Protection Officer
dell'Ordine degli Avvocati di Lecce
Avv. Andrea Lisi