DOMANDE & RISPOSTE

Cos'è il Gdpr?
È il General data protection regulation o Regolamento generale per il trattamento di dati personali n. 2016/679 entrato in vigore il 24 maggio 2016 e che sarà pienamente applicabile il 25 maggio 2018, sostituendo la direttiva 95/46/CE, detta anche direttiva privacy «madre» in quanto è la fonte giuridica da cui prendono spunto le normative nazionali, come il codice privacy italiano.

Cosa succede il 25 maggio 2018?
l Regolamento comunitario ha diretta esecuzione negli ordinamenti giuridici nazionali: cioè si applica senza necessità di attuazione con norme locali, quindi troveranno applicazione automatica le prescrizioni in esso contenute.

Ho letto che il Gdpr contiene disposizioni che rendono laboriosa l'applicazione operativa, perché non se ne è tenuto conto?
Proprio in considerazione delle molteplici innovazioni introdotte dalla riforma, il legislatore ha previsto un «periodo di grazia» di due anni consentendo alle aziende ed agli enti di adeguarsi. Per questo, sebbene il Gdpr sia entrato in vigore il 24 maggio 2016, diverrà applicabile solo il 25 maggio 2018.

Cosa cambia per la mia azienda?
Il principio fondante di questa riforma è la «responsabilizzazione» o concettuali raramente presenti nell'ordinario patrimonio culturale aziendale. Ne sono esempi: il concetto di «rischio privacy», non collimante con la tradizionale nozione di «rischio d'impresa»; la sua ponderazione che non può essere risolta semplicemente avvalendosi delle meccaniche del «risk assessment»; l'istituto della «violazione di dati personali» che non è esattamente combaciante con il «data breach» come generalmente concepito.

Sono in ritardo, cosa dovrei fare prima?
Mappare cosa si fa in azienda con i dati personali e cercare di individuare le aree più esposte sotto il profilo della delicatezza delle informazioni individuali (ad esempio, i dati sullo stato di salute sono più sensibili di mere anagrafiche), delle motivazioni d'uso (indirizzi postali a fini di corrispondenza personale producono un minore impatto rispetto ad un loro utilizzo a scopo di direct marketing), delle misure di sicurezza adottate (postazioni informatiche prive di credenziali di accesso o con credenziali di gruppo, sono maggiormente esposte, rispetto alle medesime postazioni prive di sistemi di crittografia), dei contesti (lacune registrate riguardo ad un archivio manuale risultano meno gravi di analoghe carenze nel mondo online). Quindi, concentrarsi per mettere a norma le aree più critiche, semmai avvalendosi di un esperto o di chi ha già completato questo esercizio con successo.

Quali sanzioni si rischiano?
Il Gdpr inasprisce le sanzioni

«accountability», secondo cui l'azienda o l'ente, denominati «titolari del trattamento», sono liberi di valutare come conformarsi alla norma ma rispondono della correttezza del loro operato; in aggiunta, in virtù di tale «responsabilizzazione», spetterà all'azienda dimostrare di essere conforme. Questo significa che il problema della dimostrazione della correttezza del proprio operato non sorge più solo in caso di presunto inadempimento ma anche senza alcun indizio di abusi od omissioni.

Come si può gestire al meglio la accountability?

Siccome l'adeguamento alla norma è rimesso alla valutazione dell'azienda o dell'ente, occorre che il titolare del trattamento sia in grado di effettuare valutazioni appropriate nei diversi contesti. Si tratta di una significativa sfida per le imprese sia in termini quantitativi – in quanto il Gdpr è costellato di occorrenze che presuppongono valutazioni – sia sotto il profilo qualitativo, perché questi giudizi presuppongono categorie

amministrative pecuniarie stabilendo un tetto massimo significativamente più elevato di quello fino ad oggi previsto. Per le violazioni degli obblighi del titolare e del responsabile, in particolare degli articoli 25 (privacy by design/by default) e 32 (sicurezza), la sanzione prevista può arrivare fino ad un massimo di 10 milioni di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Le sanzioni possono invece arrivare a 20 milioni di euro o al 4% del fatturato, sempre se superiore, in caso, ad esempio, di violazioni dei principi fondamentali in materia di protezione dei dati personali, dei diritti dell'interessato e per l'inosservanza degli ordini dell'autorità di controllo o degli obblighi emanati dagli Stati membri a norma del Gdpr. Il Regolamento, pur lasciando agli Stati membri la possibilità di prevedere sanzioni penali, precisa che l'irrogazione delle stesse non deve essere in contrasto con il principio del «ne bis in idem» quale interpretato dalla Corte di Giustizia Ue, che vieta un sistema a doppia sanzione e a doppio processo.