EDITORIALE

valentina.frediani@ildocumentodigitale.com

Quali conseguenze della GDPR su produttori/fornitori ICT?

I temi introdotti dall'emanazione della *General Data Protection Regulation* (GDPR) sono molteplici ed a partire da adesso fino al maggio del 2018 è opportuno analizzarli secondo un criterio prioritario. **Personalmente ritengo che i primi soggetti a doversi occupare dei risvolti pratici della GDPR dovranno essere le aziende che realizzano servizi e/o prodotti in ambito informatico**. Difatti, queste imprese potrebbero già trovarsi oggi - o comunque nel breve termine - a dover far fronte ad una richiesta specifica dei propri clienti in merito alla compliance di quanto realizzano rispetto al Regolamento Europeo.

Questo perché chi oggi investe su prodotti o servizi che possono trovare allocazione nella propria struttura per un arco temporale che possa superare il maggio 2018, ha tutto l'interesse a non dover andare incontro a situazioni "precarie" sotto il profilo della compliance, rispetto all'investimento sopportato. Al fine quindi di evitare nuovi investimenti piuttosto che affrontare le difficoltà consequenziali alla sostituzione di prodotti/servizi ICT, è naturale che Direzioni acquisti e ICT Manager portino già oggi sul tavolo delle trattative il tema privacy. Ecco che allora diviene prioritario chiedersi che cosa dovranno affrontare i produttori/fornitori del settore.

Vi sono fondamentalmente tre macro temi:

- uno strettamente collegato alle misure tecniche atte a garantire la compliance rispetto al Regolamento (privacy by design);
- il secondo, sempre di natura tecnologica, atto a verificare come un prodotto/servizio possa essere calato nella realtà aziendale di destinazione affinché vi sia l'adeguamento sotto il profilo normativo (privacy by default);
- l'ultimo inerente la contrattualistica che diviene elemento obbligatorio rispetto a quanto previsto nella GDPR.

Scorrendo il testo normativo emerge in modo molto chiaro il principio della cosiddetta *accountability* quindi l'onere del titolare di dimostrare di aver adottato quanto di sua competenza. L'assenza della tassatività di misure tecniche lascia aperto per i fornitori un ampio margine di intervento su quelli che sono gli aspetti di natura tecnologica dovendo però andare ad affrontare l'adeguamento nel rispetto dei cosiddetti 7 principi del PbD ovvero:

- intervento proattivo non reattivo - preventivare non rimediare;
- privacy by default;
- privacy incorporata nell'architettura del sistema;
- conciliazione tra massima funzionalità e rispetto dei diritti;
- protezione del ciclo di vita dei dati;
- visibilità e trasparenza;
- centralità dell'utente.

Sviluppi ed implementazioni dovranno essere effettuati parallelamente alla redazione di una documentazione tecnico-legale in grado di dimostrare, storicamente, le scelte operate e come i predetti principi sono stati applicati al fine di garantire e dimostrare l'adeguatezza rispetto alla GDPR.

È opportuno ricordare come la dimostrabilità dell'adeguamento normativo non ricada solo sotto una sfera meramente "commerciale" per i fornitori (è chiaro che non essere in regola diverrà un discrimine dal punto di vista della proponibilità sul mercato), in quanto gli stessi potranno essere corresponsabili in caso di realizzazione di prodotti/servizi non in linea con la GDPR con un rischio sanzionatorio variabile dai 10 milioni ai 20 milioni di euro o in alternativa fino al 4% del fatturato globale mondiale annuo.

Priorità quindi su questi temi, perché il mercato subirà un reale impatto dall'entrata in vigore della normativa.

Valentina Frediani