Pasquale Davide

GDPR

Regolamento generale sulla protezione dei dati

info@ict-professionals.it

Quaderni di Informatica
N°1 - Gennaio 2018

Sommario

L'articolo ricorda che a breve, e precisamente a far data dal 25 maggio 2018, entrerà in vigore la nuova normativa sulla protezione dei dati, con numerose e rilevanti novità rispetto alla precedente legge sulla privacy. Con la nuova norma si passa dalla "direttiva" al "regolamento", si passa dalle “misure minime” alle misure “idonee”, viene sancito il concetto dell’obbligatorietà dell' analisi dei rischi. Alla domanda chi è tenuto all’adeguamento al nuovo GDPR , la risposta è tutti con l'esclusione dei soli trattamenti domestici. Le sanzioni amministrative arrivano sino a 20.000.000,00 di euro o al 4% del fatturato per i gruppi aziendali internazionali. Ma nonostante sanzioni così elevate ed il fatto che siano trascorsi quasi due anni dall’approvazione del GDPR lo stato di avanzamento dei lavori in Italia è ancora molto in ritardo.

L'Autore

Pasquale Davide, m*anager, ha acquisito in circa 40 anni di esperienza sul campo, specifiche competenze nell’area delle risorse tecnologiche. Dal 1976 presso la Banca Sannitica di Benevento, e poi dal 1993 presso la Banca di Credito popolare di Torre del Greco, dove ha percorso tutta la carriera manageriale da Responsabile CED a Vice Direttore Risorse (ICT- Organizzazione - Business Continuity- Cost management- buyer office). Membro del Comitato Tecnico e del Comitato Guida del Consorzio Informatico Secservizi di Padova, ha svolto anche, e svolge tutt'ora incarichi di consulenza organizzativa, sicurezza dati e privacy per enti pubblici ed aziende private.*

Il 25 maggio 2018 il GDPR sostituirà la direttiva “nonna” 95/46/CE che aveva dato origine alla prima generazione della “Legge privacy” Italiana: ben nota 675/96, prima e il codice privacy D.lgs 196 del 30 giugno 2003 poi come seconda generazione. L’attuale corpo normativo, costituito da legge primaria e norme secondarie decadrà se il conflitto con le prescrizioni del GDPR sarà irrisolvibile.

La genesi del GDPR risale al 2012 ma la prima tappa fondamentale è stata registrata il 4 maggio 2016 con la pubblicazione sulla Gazzetta Ufficiale Europea del regolamento generale in tema di protezione dei dati personali 2016/679. Il GDPR è entrato in vigore dal 24 maggio 2016, tuttavia l’attuazione si ha a partire dal prossimo 25 maggio 2018. Il regolatore Europeo ha concesso, quindi, due anni di tempo ai Titolari e Responsabili del trattamento dati per adeguare: le normative interne, formulari, processi e strumenti di lavoro alle nuove prescrizioni.

Il nuovo regolamento, infatti, articolato e complesso ha introdotto rilevanti novità imprimendo un cambio culturale significativo nella tutela dei dati personali rispetto alle precedenti normative per lo più orientate al formalismo più che alla sostanza.

Con la nuova norma si passa dalla direttiva al regolamento. Viene rafforzato il consenso e vengono introdotti nuovi diritti che richiedono un'informativa adeguata. Sono state introdotte, inoltre, nuove categorie di dati. Si passa dalle "misure minime" alle misure "idonee": viene sancito il concetto dell'analisi dei rischi.

Il nuovo regolamento esige una maggiore responsabilità da parte del Titolare o del Responsabile del trattamento dei dati personali introducendo nuovi concetti fondamentali: *Accountability*, *privacy by design*, *privacy by default, data protection*, *impact assessment*.Tutti questi concetti hanno in comune un nuovo approccio: la protezione dei dati.

Il *data breach*, con le regole in caso di violazioni dei dati personali, richiede che le aziende si dotino di processi efficienti nel notificare la violazione avvenuta giacché l'intero processo della notifica deve esaurirsi nelle 48 ore al più tardi nelle 72 ore, in tal caso occorre giustificare il motivo del ritardo al Garante per la protezione dei dati personali.

Il diritto all'oblio dei dati nonché la cancellazione e portabilità dei dati hanno delle rilevanti ricadute sulle procedure informatiche.

L'entità organizzative con funzione pubblica (es. Comuni, città metropolitane, scuole, ordini professionali, ecc), le aziende con più di 250 dipendenti o che effettuano trattamenti dei dati personali con rischio di violazione elevato, hanno l'obbligo di nominare la figura del DPO (Data Protection Officer). Detta figura è complessa per le caratteristiche, le competenze trasversali, l'indipendenza, i compiti da espletare. È particolarmente individuabile all'interno del mercato, dunque, essendo caratterizzata da una rara professionalità.

Alla domanda chi è tenuto all'adeguamento al nuovo GDPR la risposta è tutti; sono esclusi solo i trattamenti domestici. Nell'applicabilità della norma il principio di proporzionalità fa la differenza tra le aziende.

Cambiano ruoli e responsabilità. In tale ambito va rivisto il rapporto tra Titolare, i fornitori/Responsabili ed i sub fornitori Responsabili. Gli obblighi normativi, pertanto, hanno delle ricadute significative oltre che sulle procedure informatiche anche su i contratti di outsourcing informatico e di back-office.

I Titolari e i Responsabili del trattamento dei dati personali, a circa 100 giorni dalla piena applicabilità del regolamento Europeo sulla data protection, devono fare

il punto su quanto è stato fatto in direzione delle nuove disposizioni e quali sono le novità ancora da espletare tracciando un cronoprogramma di adeguamento alla normativa.

Tale cronoprogramma deve prendere avvio dalla sensibilizzazione e formazione dei propri Rappresentanti, Collaboratori ed Associati così come prescrive l'articolo 32 comma 4 del regolamento 679/2016« […] chiunque abbia accesso ai dati personali non tratti tali dati se non istruito in tal senso dal Titolare del trattamento o dal Responsabile».

Le condizioni generali per irrogare sanzioni amministrative son cambiate. Esse arrivano sino a 20.000.000,00€ o al 4% del fatturato per i gruppi aziendali internazionali.

Ma nonostante che le sanzioni siano così elevate e che siano trascorsi quasi due anni dall'approvazione del GDPR, in Italia sembra che lo stato di avanzamento dei lavori lasci molto a desiderare.

Come espletare gli adempimenti richiesti dalla GDPR?

Costituire un gruppo di lavoro che abbia adeguate competenze per mettere in atto: misure fisiche, tecniche informatiche , misure organizzative e misure procedurali e documentali.

Il reale impegno consiste nell'organizzare la sicurezza.

Bisogna non cedere alla tentazione di fare tutto in casa, l'incidente è dietro l'angolo e solo dopo ci si rende conto dei costi derivanti della mancata conformità alle norme.

I Titolari delle aziende dovranno fare attenzione a distinguere il consulente con metodo da quelli "fotocopiatori" e bravi nel taglia & incolla.

Buon Lavoro!