PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4159 di Lunedì 22 gennaio 2018

GDPR 2016/679: oltre il 90% delle imprese è coinvolto

Mancano poco più di 200 giorni alla data in cui diventerà operativo il Regolamento Europeo sulla protezione dei dati personali.

Entro il **25 maggio 2018** sono tenuti ad adeguarsi agli adempimenti previsti dalla normativa tutti i Soggetti Pubblici e Privati che effettuano il trattamento di dati personali, archiviati in forma elettronica e/o cartacea. Tra questi, aziende, avvocati, commercialisti, organismi sanitari, istituzioni scolastiche, comuni e tutti coloro che trattano dati personali, anche mediante l'ausilio di strumenti elettronici.

Quali sono le novità rispetto al precedente D. Lgs. 196/03?

Il regolamento introduce una serie di novità in materia di obblighi, diritti e conseguenti rischi, rilevanti per le aziende dal punto di vista sia economico (sanzioni fino al 4% del fatturato worldwide) sia di immagine (possibili conseguenze di un incidente informatico che metta a rischio l'integrità o la riservatezza dei dati).

La maggior parte delle Organizzazioni si trovano nella condizione di dover soddisfare nuove esigenze tra cui:

- **la nomina di figure professionali specifiche**
- **l'istituzione di un registro di trattamento dati**

In tema di "figure professionali", il Regolamento cita una nuova funzione, quella del **DPO**.

Da ricerche effettuate dagli osservatori, alcune ricerche hanno già previsto una funzione specifica per la gestione dei dati personali trattati ma la maggior parte delle organizzazioni ancora non ha chiaro se si incorre nell'obbligo di nominare un responsabile della protezione dati.

Chi è il DPO? Sarà sempre obbligatorio nominarlo? Quanto costerà?

Innanzitutto, tranquillizziamo tutti precisando subito che il legislatore dà, per fortuna, la possibilità di individuare questa figura sia esternamente e sia internamente tra i propri dipendenti.

È importante, comunque, conoscere bene i contenuti e gli ambiti di applicazione del nuovo regolamento.

Il DPO, Data Protection Officer, ha il compito di assicurare la protezione del patrimonio informativo aziendale e dei dati personali trattati.

Per quanto concerne i requisiti richiesti dal regolamento, il Data Protection Officer dovrà essere messo in condizioni di assoluta indipendenza e in totale assenza di conflitti di interesse, dovrà possedere adeguate risorse umane e finanziarie, competenze informatiche e un'ottima conoscenza della normativa sulla privacy. Tale incarico potrà essere affidato sia ad un dipendente interno dell'azienda sia ad una figura esterna tramite un contratto di servizi.

La nomina del DPO è **obbligatoria**:

- se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali;
- se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su **larga scala** (ad esempio *tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale, utilizzo tessere fedeltà esercizi commerciali come le farmacie*; *occuparsi del funzionamento di una rete di telecomunicazioni; tracciamento dell'ubicazione; i programmi di fidelizzazione; utilizzo di un sistema di videosorveglianza; reindirizzamento di messaggi di posta, attività di marketing basate sull'analisi dei dati raccolti, automobili intelligenti, dispositivi per la domotica; ecc.)*
- se le attività principali del titolare o del responsabile consistono nel trattamento su **larga scala** (*notevole quantità di dati su scala regionale, nazionale, sovranazionale*) di categorie particolari di dati (ad esempio *dati sanitari)* o di dati personali relativi a condanne penali e reati.

Cosa contiene il Registro dei trattamenti? Quando è necessario?

L'articolo 30 del Regolamento fa riferimento a questo importante strumento di rilevazione delle attività: il **registro delle attività di trattamento dei dati personali**.

Tenuto anche in formato elettronico dal Titolare del trattamento dei dati, tale registro dovrà essere messo a disposizione dell'Autorità Garante qualora lo richieda, così come è previsto dal Regolamento stesso.

Per chi vige l'obbligo?

L'obbligo di redazione e adozione del registro non è generale: infatti il par. 5 dell'art. 30 specifica che la tenuta del registro **non** compete "alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10."

C'è, però, da considerare che la predisposizione del registro non deve essere vista solo come un obbligo perché non solo costituisce uno strumento di pianificazione e controllo delle attività ma permette anche di condividere le informazioni con l'intera organizzazione.

In quest'ottica, **Blumatica** sta implementando un innovativo sistema di gestione che permetterà di adeguare qualunque tipo di Organizzazione ai nuovi requisiti privacy, rivolgendosi sia al consulente che presta il proprio servizio ad un numero indefinito di

aziende sia alla grande Organizzazione che intende gestire all'interno il trattamento dati.

Una check-list di autovalutazione consentirà di individuare tutte le operazioni da fare per allinearsi ai nuovi requisiti normativi.

Per maggiori info clicca qui

---

www.puntosicuro.it