INDUSTRIA 4.0

Siete in regola con il Gdpr?

Dal 25 maggio 2018 sarà operativa la nuova normativa europea relativa alla protezione dei dati personali (Gdpr, General data protection regulation) pubblicata il 4 maggio 2016 ed entrata in vigore il 25 maggio dello stesso anno. L'obiettivo del regolamento è di uniformare le normative dei diversi Paesi membri dell'Unione Europea in un'unica norma generale per garantire la privacy delle persone fisiche all'interno del mercato Europeo e rimuovere gli ostacoli alla circolazione dei dati personali. La normativa tutela il diritto di ogni persona fisica di essere sicura che i propri dati vengano utilizzati esclusivamente per gli scopi e le finalità a cui ha dato il proprio consenso. Ma quali sono le parole chiave principali di questa nuova normativa? Eccole di seguito in un elenco con relativa breve descrizione che può essere d'aiuto alle aziende per comprendere le attività da attuare.

Responsabilizzazione o accountability
Ogni azienda e il titolare del trattamento dei dati hanno il compito di assicurare, ed essere in grado di provare, il rispetto dei principi applicati dal trattamento dei dati personali Gdpr. A differenza della norma sulla privacy italiana attualmente in vigore, che richiede una condotta basata sull'attuazione delle misure minime di sicurezza per la protezione dei dati, la nuova normativa europea impone invece una condotta proattiva tale da dimostrare la concreta adozione delle misure necessarie ad assicurare l'applicazione del regolamento stesso.

A fine maggio scatta la nuova legge europea sulla privacy. Interessa tutte le aziende, che rischiano multe sino al 4% del fatturato se non si mettono in regola. Ecco le parole chiave per scoprire la General data protection regulation

Dpo (Data Protection Officer) o Responsabile della protezione dei dati
Persona o organo addetto alla sorveglianza in merito al sistema di gestione dei dati conforme al Gdpr. Gode di piena autonomia sia per risorse umane che finanziarie, che devono essere utilizzate per implementare tutte le disposizioni necessarie al rispetto della norma. Riferisce direttamente al titolare dell'azienda, non sono necessari attestati formali a dimostrazione delle competenze professionali e non è necessaria l'iscrizione all'albo dei «Responsabili della protezione dei dati». È obbligatorio nelle realtà con più di 250 addetti, oppure in caso di trattamenti particolarmente delicati e rischiosi.

Dpia (Data protection impact assessment) o valutazione dell'impatto sulla protezione dei dati
Insieme di controlli per la valutazione dei rischi derivanti dal trattamento dei dati personali per i diritti e le libertà degli interessati; obbligatoria quando si presume un rischio elevato, è comunque consigliata in tutti i casi. I contenuti sono dettagliatamente indicati all'articolo 30 Gdpr.

Registro dei trattamenti dei dati
Obbligatorio nelle realtà con più di 250 addetti, oppure in caso di trattamenti particolarmente delicati e rischiosi, è consigliato perché può costituire parte integrante di un sistema di corretta gestione dei dati personali.

Titolare del trattamento
Azienda o ente che ha potere decisionale sull'utilizzo e la modalità di gestione dei dati raccolti.

Privacy by default e by design
Necessità di configurare il trattamento dei dati su scopo del trattamento e tempo di detenzione dei dati, prevedendo fin dall'inizio le garanzie indispensabili, al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati.

Data breach o Violazione dei dati
È qualsiasi violazione dei dati trattati come distruzione, perdita, accesso o divulgazione non autorizzati. È necessario che l'azienda notifichi alle autorità di controllo le violazioni ai dati personali, di cui è venuta a conoscenza, entro 72 ore se si ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. La notifica deve essere comunicata anche ai proprietari dei dati violati. In ogni caso i titolari del trattamento dei dati dovranno documentare le violazioni subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché i provvedimenti adottati per impedire nuove violazioni.

Quali sono i dati tutelati dal Gdpr?
La normativa tutela i dati personali, ovvero tutti quei dati che identificano una persona fisica e possono fornire dettagli sulle sue caratteristiche (come abitudini, stile di vita, relazioni personali, stato di salute, situazione economica, geolocalizzazione); quelli anagrafici (nome e cognome, foto, codice fiscale…); quelli sensibili (origine razziale ed etnica, convinzioni religiose, politiche, o di altro genere; giudiziari (che rivelano l'esistenza di determinati provvedimenti a soggetti, con iscrizione nel casellario giudiziale). I dati si considerano personali se consentono l'identificazione della persona fisica direttamente, ma anche indirettamente, tramite l'incrocio dell'informazione con altre informazioni. Il dato personale è un concetto dinamico che va sempre riferito al contesto: ne è un esempio la tecnica di tracciamento per poter identificare i navigatori online. Infatti, i cookie sono considerati dati personali. Sono dati personali gli indirizzi e-mail, l'identità digitale, l'account name o nickname. Anche le informazioni riguardanti la vita professionale e pubblica di una persona sono dati personali, definendo quindi che non c'è confine nella tutela dei diritti delle persone giuridiche. I primi dati a dover essere tutelati sono quelli dei propri dipendenti e collaboratori: Certificazione Unica, cedolini degli stipendi, appartenenza ai sindacati sono un esempio. Seguono dati bancari, non solo di dipendenti, ma anche di azienda, fornitori, clienti. Qualsiasi azienda ormai tratta tutti questi dati digitalmente, tutti abbiamo il dovere di proteggerli per la responsabilità nei confronti di coloro che ce li hanno affidati.

Quali sono i diritti degli interessati?
I soggetti hanno diritto di poter accedere anche in autonomia ai propri dati, di ricevere una copia dei dati personali oggetto di trattamento, di chiedere la cancellazione dei propri dati («diritto all'oblio»), di ricevere entro 30 giorni dalla raccolta dei dati l'informativa con le specifiche sulle finalità del trattamento, quali informazioni sono mantenute, da chi sono trattate e per quanto tempo sono conservate.

Perché essere in regola?
Le sanzioni, a differenza della vecchia norma, possono arrivare fino al 4% del fatturato o fino a 20 milioni di euro (art. 83 e 84 Gdpr). I danni, in caso di violazione dei dati, non sono solo economici, ma anche di immagine, dato che è necessario notificare ai proprietari dei dati la violazione subita. Essere in regola con la norma vuol dire dare garanzia di lavorare in qualità e rispettare i dati e le informazioni ricevute, una sicurezza e valore aggiunto in più per il proprio business.

Il vostro sistema informativo è in regola?
Le applicazioni software che utilizzate per raccogliere i dati rispondono alla richiesta della normativa del diritto all'oblio (cancellazione) dei dati di un utente? I vostri sistemi operativi e antivirus sono aggiornati? Una delle prime cause di accesso illecito è dovuto a sistemi obsoleti e non aggiornati alle ultime release. Il vostro sistema informativo è dotato di una soluzione per la protezione della rete? I firewall, già obbligatori con la precedente normativa, sono diventati dispositivi necessari per la protezione perimetrale della rete aziendale. È però fondamentale che i firewall siano dotati di tutti i componenti di intrusion prevention: se sono presenti rispondete alla richiesta del Gdpr di essere proattivi.

La vostra soluzione risiede in cloud?
Il fornitore del cloud vi ha già fornito la documentazione aggiornata relativa al nuovo trattamento dei dati?
Un buon metodo per alleggerirsi dalle attività di messa in sicurezza della propria infrastruttura è l'utilizzo del cloud, sia nella fornitura di Platform as a service (per l'hosting) sia nella fornitura di Software as a service (soluzioni gestionali e applicative fornite con servizi in cloud). Attenzione, però, che il fornitore dei servizi cloud fornisca la garanzia che l'ambiente sia compliance con quanto richiesto dal Gdpr!

Sonia Zanon,
Centro di Consulenza Aziendale
Nav-lab, esperta in digitale alla Ingest