A.M.P.I. Associazione delle Micro, Piccole e Medie Imprese della Produzione e dei Servizi
Piazza Repubblica, 29/A- 30014 Cavarzere (VE)
Tel. 0426/51703 Fax 0426/52065
C.F. e P.IVA 03806600270
www.associazioneampi.it ampi@associazioneampi.it
associata CNA Venezia

Il nuovo Regolamento Europeo della privacy,

GDPR in azienda: come fare per mettersi in regola

Il nuovo regolamento europeo rivoluziona il trattamento dei dati personali e la tutela della privacy in ambito professionale. Le aziende sono chiamate ad adottarne le direttive entro il 25 maggio 2018: vediamo come.

Si chiama GDPR (General Data Protection Regulation) e segna il prossimo importante adeguamento in termini di compliance per tutte le aziende europee, indipendentemente dalle loro dimensioni. Si tratta del nuovo Regolamento Generale sulla Protezione dei Dati, ossia un insieme di norme e linee guida che, a partire dal 25 maggio 2018, tutte le realtà professionali dovranno rispettare con l'obiettivo di rendere omogenee e rafforzare le modalità di trattamento dei dati personali nella UE.

Questo significa, in tempi ormai davvero brevi, consolidare le misure per la tutela della privacy seguendo i dettami del GDPR, rispondendo al contempo ad un'esigenza di protezione e sicurezza dei dati sentita a livello globale e legata a doppio nodo all'emergere di minacce informatiche sempre più complesse.

GDPR: cosa è?

Il nuovo Regolamento si propone di restituire ai cittadini europei il pieno controllo sui propri dati personali, un diritto spesso ostacolato da legislazioni nazionali differenti e da scenari tecnologici che a volte sfuggono all'attuale normativa. Per questo, adottare regole uniformi diventa l'unica strada percorribile. Ecco perché tutte le aziende sono chiamate ad adeguarsi, dimostrando di operare in conformità a quanto previsto dal GDPR.

L'obbligo di osservanza delle direttive è imposto anche alle imprese con sede legale al di fuori del territorio europeo ma che, nella loro attività, si trovano a gestire o trattare dati personali di chi risiede nello spazio UE.

Conformità al GDPR: cosa fare?
DPO in azienda: ruolo e responsabilità

Innanzitutto, il regolamento prevede che ogni azienda nomini un Responsabile della Protezione dei Dati (RPD) – nel Regolamento indicato come **Data Protection Officer (DPO)** – adeguatamente formato per assolvere al compito nel migliore dei modi e a cui spetta l'incarico di fornire informazioni relative alla propria attività ai diretti interessati, siano essi i collaboratori della società, i fornitori oppure i clienti.

Il presupposto di base per un trattamento dei dati personali a norma di legge, infatti, è che l'azienda-titolare del trattamento ne abbia ottenuto il consenso libero, specifico ed informato. Ecco perché il GDPR detta specifiche linee guida al fine di garantire questo fondamentale passaggio, dettagliando quali tipologie di informazioni minime è necessario offrire al soggetto al fine di ottenere il suo consenso al trattamento.

Divise in sei categorie, si tratta di: identità del titolare; scopo delle operazioni di trattamento per le quali è richiesto il consenso; tipo di dati raccolti e trattati; esistenza del diritto di revoca del consenso; uso dei dati per le decisioni basate su elaborazione automatica (inclusa profilazione); nel caso di trasferimento verso paesi terzi, possibili rischi in assenza di garanzie e scelte appropriate.

Come ottenere il consenso al trattamento

È poi necessario procedere alla tutela dei dati mediante impiego di crittografia, così da renderli non fruibili a soggetti non autorizzati. Bisogna inoltre garantire che, in seguito a un eventuale problema di natura fisica o tecnica, l'accesso alle informazioni venga ristabilito in modo tempestivo.

Per essere compliant, quindi, si devono rispettare procedure standard di protezione (pseudo- nimizzazione e cifratura dati) e prevedere assessment delle misure tecniche e organizzative adottate, che dimostrino la capacità di assicurare riservatezza, integrità, disponibilità, resilienza dei sistemi e dei servizi di trattamento, nonché ripristino tempestivo della disponibilità e dell'accesso dei dati personali in caso di incidente fisico o tecnico.

Il GDPR introduce infatti il principio di accountability per tutte le fasi del trattamento. Questo significa adottare soluzioni e strumenti che garantiscano non soltanto la protezione del dato ma anche il controllo, la verifica e l'analisi delle procedure.

Nel caso di una fuga di dati, che si può verificare tramite manomissione, attacco esterno o in modo accidentale, è poi obbligatorio darne avviso tempestivo (entro 72 ore dall'identificazione del problema) all'autorità garante. Eventuali ritardi andranno giustificati.

Per le realtà professionali che contano più di 250 dipendenti vige infine l'obbligo di redigere un registro delle attività con i dettagli sulle policy aziendali attuate in materia di privacy, sulle procedure adottate e sugli standard di sicurezza vantati.

Cosa annotare nel registro delle attività

GDPR compliant: come diventarlo?

Al fine di assicurare la conformità a quanto previsto dal GDPR, nonostante i tempi ormai siano piuttosto stretti, i passi da compiere sono dunque molti ma imprescindibili. Oltre a contribuire nel centrare gli obiettivi del regolamento, infatti, si eviterà di incappare in sanzioni che, per la mancata compliance, possono arrivare fino al 4% del fatturato.

In ogni caso, è bene non adottare soluzioni improvvisate e avvalersi di consulenti e partner IT preparati e certificati per stilare il piano d'azione migliore e ottimizzare gli investimenti necessari. Se infatti è vero che il GDPR rimette le persone al centro (riconoscendo il pieno diritto alla trasparenza del trattamento dati) è anche vero che tutto questo è ottenibile solo attraverso l'impiego di sistemi e soluzioni altamente affidabili e ad elevato contenuto tecnologico.

Tecnicamente, il primo passo è sostituire le soluzioni di archiviazione locale dei dati con sistemi che centralizzino sia la gestione delle autorizzazioni sia l'accesso ai dati. In altre parole, non sarà più possibile conservare i file esclusivamente su un computer o un disco locale, bensì sarà bene optare per una più avanzata e affidabile soluzione di storage e backup: i sistemi cloud costituiscono a tal fine una delle migliori alternative disponibili, grazie anche (ma non solo) alla ridondanza dei sistemi impiegati.

Affidarsi a fornitori di servizi cloud che certificano la localizzazione all'interno dell'Unione Europea è un'altra scelta possibile, poiché ci si assicura che la gestione delle informazioni avverrà in conformità con il regolamento, nel pieno rispetto degli standard e dei requisiti stabiliti a livello UE.

Lo stesso vale per i Trust Service Provider che si occupano di certificare l'identità digitale mediante strumenti come la firma elettronica o lo SPID(Sistema Pubblico di Identità Digitale).

Pronti al GDPR: entro quando?

Il testo parla chiaro: a partire dal 25 maggio 2018 il GDPR andrà definitivamente a sostituire le precedenti direttive sulla protezione dei dati. Sarà dunque scardinato e profondamente modificato uno scenario consolidato da anni, che – complice l'evoluzione del mondo online – oggi risulta insufficiente nel rispondere alle nuove esigenze, non soltanto di privacy ma anche di cyber security.

Come sempre, quando ci si trova di fronte a un cambiamento importante, possono insorgere dubbi legittimi e alcune comprensibili difficoltà. Fortunatamente è possibile contare sul supporto di partner certificati e pronti a mettere le proprie competenze al servizio di chi ne ha necessità.

Orientamenti UE sul nuovo GDPR

In tema di piattaforme cloud e soluzioni per lo storage dei dati, a livello europeo il CISPE (Cloud Infrastructure Services Providers in Europe) raggruppa alcuni dei provider che assicurano il pieno rispetto delle regole: tra questi c'è anche un importante player italiano, Aruba, che tramite l'adozione di un codice di condotta garantisce ai propri clienti che le informazioni vengono salvate e trattate esclusivamente all'interno dei territori UE/SEE, senza mai essere cedute a soggetti terzi.

Come già detto nelle precedenti circolari, stiamo attivandoci per trovare una soluzione per gli associati. Gli interessati possono fare riferimento alla nostra segreteria.

Il Presidente

Dott. Giorgio Ferro

tratto da www.pmi.it