aetherna

informa

GDPR

IL NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY

Cosa

Il GDPR (General Data Protection Regulation) è il Regolamento con il quale la Commissione europea intende rafforzare e armonizzare la protezione dei dati personali entro i confini dell'UE, sostituendo la direttiva sulla protezione dei dati (ufficialmente Direttiva 95/46/EC) istituita nel 1995.
Si tratta di un importante passo avanti in tema di standardizzazione delle politiche europee e di protezione dei dati a livello continentale.

Quando

Il nuovo Regolamento UE 2016/679 ("il Regolamento") è entrato in vigore il 24 maggio 2016.
Le norme saranno applicabili dal 25 maggio 2018 e il tempo a disposizione per capire la strategia migliore da applicare e metterla in atto non è molto.

Obiettivo

Gli obiettivi principali sono quelli di consolidare i diritti della privacy dei cittadini dell'UE, ripristinare la fiducia nelle attività online e fornire maggiore protezione ai dati dei clienti, esigendo l'adozione di nuovi processi e controlli.
Al fine di semplificare il contesto normativo che riguarda gli affari internazionali, la nuova norma, più moderna e trasparente, avrà un'unica visione in tutta l'Unione Europea, sostituendo l'attuale discontinuità legislativa dei singoli Paesi.

Modifiche

Il Regolamento porterà una serie di innovazioni non solo per il singolo cittadino, ma anche per aziende, enti pubblici, libere professioni e associazioni.
Cambierà l'estensione della giurisdizione a tutte le società che trattano dati personali di soggetti risiedenti nell'Unione Europea, indipendentemente dalla localizzazione geografica dell'azienda o dal luogo in cui i dati vengono gestiti ed elaborati.
Amministrare la "privacy" all'interno dell'organizzazione non potrà più essere un semplice adempimento ai singoli obblighi normativi (a volte più formale che sostanziale): il GDPR implicherà di impostare un processo, analizzare i rischi e gestire, nel tempo, con continuità e nel fermo rispetto dei diritti di ogni individuo, i dati personali trattati.

Diritti dell'individuo

Privacy personale

- Accedere ai propri dati personali
- Correggere errori nei propri dati personali
- Cancellare i propri dati personali
- Contestare l'elaborazione dei propri dati personali
- Esportare dati personali

Doveri delle aziende

Controlli e notifiche

- Proteggere i dati personali con misure di sicurezza appropriate
- Segnalare alle autorità le violazioni dei dati personali
- Ottenere consenso appropriato per l'elaborazione dei dati
- Conservare la documentazione dettagliata sull'elaborazione dei dati

Criteri di trasparenza

- Fornire avvisi chiari sulla raccolta dati
- Evidenziare gli scopi dell'elaborazione e i casi di utilizzo
- Definire i criteri di conservazione e di eliminazione dei dati

IT e Formazione

- Formare personale e dipendenti che si occupano di privacy
- Controllare e aggiornare i criteri relativi ai dati
- Avvalersi di un responsabile della protezione dei dati (se necessario)
- Creare e gestire contratti fornitore conformi

Elementi principali

Nell'art.32 viene richiesto alle organizzazioni di adottare misure di sicurezza adeguate tramite la *cifratura dei dati personali* e *la capacità di assicurare l'attuale riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati.*
Se si dovesse verificare la violazione dei dati personali, l'art.33 stabilisce che l'azienda ha l'obbligo di inviarne comunicazione all'autorità di controllo entro 72 ore dalla presa d'atto dell'infrazione. Tuttavia, l'organizzazione dovrà comunicarne notifica di tale violazione agli individui i cui dati sono stati violati.
Se non vengono implementate le giuste tecnologie per la protezione dei dati personali, l'art.34 indica il rischio di perdite finanziarie, sia dirette (sanzioni da versare all'auorità di controllo), che indirette (danni alla reputazione, perdita di fiducia e di rispetto da parte dei clienti).

Sanzioni

Se non rispettato, il nuovo Regolamento sarà causa di severe sanzioni, con multe fino al 4% del fatturato globale annuo o a 20 milioni di euro, a seconda di quale sia la cifra maggiore tra le due. Tuttavia, le conseguenze non saranno solo economiche: il mancato rispetto delle nuove norme avrà anche ripercussioni sulla reputazione e sull'immagine della compagnia, che non verrà considerata come attenta alla privacy degli utenti e ai loro dati sensibili.

Come mettersi in regola

Per verificare l'aderenza dei propri processi alla normativa si possono analizzare quattro aspetti chiave:

1. **ricerca**: la capacità di identificare dei dati personali presenti in azienda e la loro dislocazione;
2. **gestione**: il governo delle modalità in cui i dati sono acceduti e utilizzati;
3. **protezione**: l'impostazione di controlli di sicurezza per prevenire, intercettare e rispondere a vulnerabilità e furti di dati;
4. **documentazione**: la capacità, come richiesto dalla normativa, di rispondere a richieste di dati e di relazionare in modo puntuale e tempestivo su furti di dati.

Sebbene la nuova legge non prescriva una tipologia specifica di controllo tecnico, accenna diverse volte alla cifratura come metodo di protezione dei dati personali, in quanto li rende illeggibili agli occhi degli utenti non autorizzati.
Il 57% dei casi di violazione dei dati è dovuto ad hacker o malware, mentre il 23% deriva dalla divulgazione non intenzionale (errore umano).Per essere pronti ad affrontare le modifiche apportate dal Regolamento, occorre iniziare a prendere in considerazione l'uso di cifratura e tecnologie antimalware.

Proteggere i sistemi da queste minacce è un ottimo punto di partenza.
Le fasi da intraprendere sono tre:

1. **Bloccare le principali cause di perdita dei dati**
2. **Bloccare le minacce alla soglia del perimetro di rete**
3. **Impedire gli errori umani**

Non sai come fare? Contatta subito Aetherna!

Per ulteriori informazioni sul Regolamento, Aetherna vi invita a consultare:

1. Q&A on EU Data Protection Reform. Commissione europea, 21 dicembre 2015
2. Q&A: new EU rules on data protection put the citizen back in the driving seat. Parlamento europeo. 1 giugno 2016
3. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio. mercoledì 27 aprile 2016
4. 2016 Data Breaches - Privacy Rights Clearinghouse

Contatta Aetherna:

marketing@aetherna.com
800.978539 | 02.8936781

www.aetherna.com

Segui Aetherna su