https://eugdpr.org/the-regulation/, 17-11-2018

Cambiamenti chiave GDPR

Una panoramica delle principali modifiche apportate al GDPR e in che modo differiscono dalla precedente direttiva

L'obiettivo del GDPR è quello di proteggere tutti i cittadini dell'UE dalla privacy e dalle violazioni dei dati nel mondo odierno basato sui dati. Sebbene i principi chiave della privacy dei dati siano ancora fedeli alla direttiva precedente, sono state proposte molte modifiche alle politiche di regolamentazione; di seguito sono riportati i punti chiave del GDPR e informazioni sugli impatti che avrà sul business.

Aumento dell'ambito territoriale (applicabilità extraterritoriale)

Probabilmente il più grande cambiamento nel panorama normativo della privacy dei dati viene fornito con l'estesa giurisdizione del GDPR, in quanto si applica a tutte le società che trattano i dati personali degli interessati residenti nell'Unione, indipendentemente dalla sede della società. In precedenza, l'applicabilità territoriale della direttiva era ambigua e si riferiva al processo dei dati "nel contesto di uno stabilimento". Questo argomento è emerso in una serie di casi giudiziari di alto profilo. GDPR rende molto chiara la sua applicabilità - si applica al trattamento dei dati personali da parte dei responsabili del trattamento e dei responsabili del trattamento nell'UE, indipendentemente dal fatto che l'elaborazione avvenga nell'UE o meno. Il GDPR si applica anche al trattamento dei dati personali degli interessati nell'UE da un responsabile del trattamento o un incaricato del trattamento non stabilito nell'UE, dove le attività riguardano: offrire beni o servizi ai cittadini dell'UE (indipendentemente dal fatto che il pagamento sia richiesto) e il monitoraggio dei comportamenti che avvengono all'interno dell'UE. Anche le imprese non UE che trattano i dati dei cittadini dell'UE devono nominare un rappresentante nell'UE.

Sanzioni Le

organizzazioni che violano il GDPR possono essere multate fino al 4% del fatturato globale annuale o 20 milioni di euro (a seconda di quale sia maggiore). Questa è la sanzione massima che può essere imposta per le violazioni più gravi, ad esempio non avendo un sufficiente consenso del cliente per elaborare i dati o violare il nucleo della privacy in base ai concetti di design. Esiste un approccio a più livelli per le ammende, ad esempio una società può essere multata al 2% per non aver ordinato i propri registri (articolo 28), non notificando l'autorità di supervisione e l'interessato in caso di violazione o non effettuando la valutazione d'impatto. È importante notare che queste regole si applicano sia ai controller che ai processori, il che significa che le "nuvole" non sono esenti dall'applicazione di GDPR.

Consenso

Le condizioni per il consenso sono state rafforzate e le aziende non sono più in grado di utilizzare termini e condizioni lunghi illeggibili pieni di legalese. La richiesta di consenso deve essere fornita in forma intelligibile e facilmente accessibile, con lo scopo di trattamento dei dati allegato a tale consenso. Il consenso deve essere chiaro e distinguibile da altre questioni e fornito in una forma intelligibile e facilmente accessibile, utilizzando un linguaggio chiaro e chiaro. Deve essere altrettanto facile ritirare il consenso, quanto farlo.

Diritti sull'oggetto dei dati

Notifica di violazione Ai sensi del GDPR, le notifiche di violazione sono ora obbligatorie in tutti gli Stati membri in cui una violazione dei dati può "comportare un rischio per i diritti e le libertà delle

persone". Questo deve essere fatto entro 72 ore dalla prima conoscenza della violazione. I processori di dati sono inoltre tenuti a notificare i propri clienti, i responsabili del trattamento, "senza indebito ritardo" dopo aver preso conoscenza di una violazione dei dati.

Diritto di accesso

Parte dei diritti ampliati delle persone interessate dal GDPR è il diritto per gli interessati di ottenere dal responsabile del trattamento la conferma dell'esistenza o meno di dati personali che li riguardano, dove e per quale scopo. Inoltre, il responsabile del trattamento fornisce una copia dei dati personali, a titolo gratuito, in formato elettronico. Questo cambiamento è un cambiamento radicale nella trasparenza dei dati e nella responsabilizzazione degli interessati.

Diritto ad essere dimenticato

Conosciuto anche come cancellazione dei dati, il diritto all'oblio autorizza l'interessato a far sì che il responsabile del trattamento cancelli i suoi dati personali, cessare l'ulteriore diffusione dei dati e potenzialmente impedire a terzi di elaborare i dati. Le condizioni per la cancellazione, come indicato nell'articolo 17, includono i dati non più pertinenti ai fini originali per il trattamento o un interessato che ritira il consenso. Va anche notato che questo diritto richiede ai responsabili del trattamento di confrontare i diritti dei soggetti con "l'interesse pubblico nella disponibilità dei dati" quando prendono in considerazione tali richieste.

Portabilità dei dati

GDPR introduce la portabilità dei dati - il diritto per l'interessato di ricevere i dati personali che li riguardano - che hanno precedentemente fornito in un "formato comunemente utilizzabile e leggibile dalla macchina" e ha il diritto di trasmettere tali dati a un altro controllore.

Privacy per design La

privacy per design come concetto esiste da anni, ma sta diventando parte di un requisito legale solo con il GDPR. Al suo interno, privacy by design richiede l'inclusione della protezione dei dati fin dall'inizio della progettazione dei sistemi, piuttosto che un'aggiunta. Più specificamente, "Il responsabile del trattamento deve ... attuare le misure tecniche e organizzative appropriate ... in modo efficace ... al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati". L'articolo 23 prevede che i responsabili del trattamento conservino e elaborino solo i dati assolutamente necessari per l'adempimento dei propri compiti (riduzione dei dati), nonché la limitazione dell'accesso ai dati personali a coloro che devono espletare l'elaborazione.

Responsabili della protezione dei dati

Secondo GDPR non è necessario presentare notifiche / registrazioni a ciascun DPA locale delle attività di elaborazione dei dati, né è richiesto di notificare / ottenere l'approvazione per i trasferimenti in base alle Clausole contrattuali tipo (MCC). Esistono invece requisiti interni per la conservazione dei documenti, come spiegato di seguito, e l'incarico di DPO è obbligatorio solo per i controllori ei processori le cui attività principali consistono in operazioni di trattamento che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala o di categorie speciali di dati o dati relativi a condanne penali e reati. È importante sottolineare che il responsabile della protezione dei dati:

- Deve essere nominato sulla base delle qualità professionali e, in particolare, delle conoscenze specializzate in materia di diritto e pratiche in materia di protezione dei dati
- Può essere un membro dello staff o un fornitore di servizi esterno
- I dettagli di contatto devono essere forniti al DPA pertinente
- Deve essere fornito con risorse adeguate per svolgere i propri compiti e mantenere le proprie conoscenze specialistiche
- Deve riferire direttamente al più alto livello di gestione
- Non deve svolgere altri compiti che potrebbero causare un conflitto di interessi.