

GDPR: le Implicazioni per le Imprese

Scritto da Administrator

Giovedì 09 Novembre 2017 11:39 - Ultimo aggiornamento Giovedì 09 Novembre 2017 11:56



Il regolamento generale sulla protezione dei dati (GDPR) è un'iniziativa dell'UE che entrerà in vigore il 25 maggio 2018.

Il GDPR introduce variazioni di vasta portata alla legislazione in materia di protezione dei dati e, se non hanno ancora iniziato, è indispensabile che le imprese inizino a compiere passi verso la conformità.

Quali sono le principali modifiche?

Il GDPR segue un approccio simile alla legislazione esistente in materia di protezione dei dati, tuttavia, ci sono alcune modifiche sostanziali.

Multe più severe

Il GDPR aumenta notevolmente il livello delle ammende che possono essere imposte. Può

GDPR: le Implicazioni per le Imprese

Scritto da Administrator

Giovedì 09 Novembre 2017 11:39 - Ultimo aggiornamento Giovedì 09 Novembre 2017 11:56

essere inflitta una multa fino a 20 milioni di euro, pari al 4% del fatturato globale, qualora sia superiore, per violazioni più gravi, ad esempio una violazione dei principi fondamentali di protezione dei dati o una violazione delle restrizioni internazionali di trasferimento.

Una multa fino a 10 milioni di euro, pari al 2% del fatturato totale a livello mondiale, qualora sia superiore, si applicherà a reati meno gravi, come il mancato mantenimento di un registro di elaborazione dati.

Scopo

Tutte le imprese, anche quelle situate al di fuori dell'UE, devono rispettare il GDPR in cui offrono beni o servizi a persone all'interno dell'UE o controllano l'attività delle persone all'interno dell'UE (ad esempio, profiling internet).

Requisito di responsabilità

Il GDPR introduce un obbligo ai responsabili e ai processori di dati di mostrare come rispettano i principi della protezione dei dati. Ciò include la creazione e la manutenzione dei registri di elaborazione dati. Se non è già in atto, devono essere adottate misure di governance globali per ridurre al minimo il rischio di una violazione e salvaguardare la protezione dei dati personali.

Misure appropriate comprendono le valutazioni dell'impatto sulla privacy per l'elaborazione ad alto rischio e le misure per garantire che la protezione dei dati sia incorporata "per disegno e per impostazione predefinita" piuttosto che essere un rimedio.

Un elemento di responsabilità è sempre stato parte integrante della legge sulla protezione dei dati, ma il GDPR pone maggiore attenzione su questo e le imprese dovrebbero assicurare che le politiche esistenti e la documentazione siano sufficienti a soddisfare i nuovi requisiti.

Un esempio primario di questa maggiore attenzione è che i controllori dei dati devono notificare all'Ufficio di Commissariato delle Informazioni entro 72 ore dalla conoscenza di una violazione dei dati che costituisce un rischio per i soggetti interessati.

Processori di dati

Attualmente, i processori di dati non hanno alcun obbligo diretto (ad eccezione del tramite del responsabile del trattamento) e il responsabile del trattamento è responsabile di qualsiasi violazione commessa dal suo processore.

Il GDPR impone obblighi specifici nei confronti dei processori di dati, incluso l'obbligo di implementare adeguati standard di sicurezza, assicurare una registrazione adeguata e informare il responsabile del trattamento di eventuali violazioni.

I processori di dati saranno ora esposti a multe regolamentari o richieste private da parte di individui in caso di violazione.

Il GDPR prevede inoltre una serie di disposizioni che devono essere incluse in tutti i contratti che prevedono l'elaborazione di dati personali. Questo aumento di oneri regolamentari e l'esposizione al rischio possono comportare una modifica degli accordi commerciali esistenti e le imprese dovrebbero dialogare con i fornitori interessati.

Ufficiali di protezione dei dati (DPO)

In alcune circostanze, un DPO dovrà essere designato dal controllore o dal processore. Ciò si applica principalmente quando l'elaborazione prevede un monitoraggio regolare e sistematico dei dati su larga scala o al settore pubblico. Il DPO deve avere sufficienti conoscenze per svolgere il ruolo e un unico DPO può essere designato per un gruppo di imprese.

Consenso

Laddove l'elaborazione si basa sul consenso, il responsabile del trattamento sarà tenuto a dimostrare che l'autorizzazione è stata conferita dall'individuo e l'opportunità di revocare il consenso deve essere resa facile come la concessione del consenso.

GDPR: le Implicazioni per le Imprese

Scritto da Administrator

Giovedì 09 Novembre 2017 11:39 - Ultimo aggiornamento Giovedì 09 Novembre 2017 11:56

Non esiste un aumento del consenso a livello di GDPR e pertanto le imprese devono garantire che i consensi preesistenti siano conformi al GDPR. Di conseguenza, alcune imprese possono cercare di allontanarsi dall'uso del consenso e cercare di contare su una base giuridica alternativa, come l'esecuzione di un contratto o un legittimo interesse del titolare del trattamento.

Diritti dei soggetti dei dati

I diritti degli interessati sono stati estesi, come il diritto di essere "dimenticato", quando un individuo può richiedere la cancellazione dei propri dati quando si applicano determinati motivi.

Esiste anche il diritto di limitare l'elaborazione in alcune circostanze, unitamente a un nuovo diritto di fornire i dati personali ai soggetti dati in modo da poter essere facilmente trasferiti (indicati come "portabilità dei dati").

Le parti dovranno assicurarsi di avere dei processi in atto per soddisfare l'esercizio di tali diritti.

Cosa devono fare le imprese adesso?

Se non lo fanno già, tutte le imprese, grandi e piccole, dovrebbero valutare la loro interazione con i dati personali e come il GDPR abbia un impatto su di loro e sul settore in cui operano, chiedendo anche la [consulenza GDPR](#) di studi specializzati.

Dato il livello di cambiamento che può essere richiesto, la scadenza del maggio 2018 potrebbe arrivare molto prima di quanto previsto.