TOSHIBA
Leading Innovation

GDPR: COSA COMPORTA PER LA VOSTRA AZIENDA

TOGETHER INFORMATION

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
COSA COMPORTA PER LA VOSTRA AZIENDA?

Il nuovo Regolamento Generale sulla Protezione dei Dati (GDPR) che entrerà in vigore a partire dal 25 maggio 2018, interesserà le attività delle aziende su scala globale. Benché si tratti di una direttiva UE, che molto probabilmente verrà adottata anche dagli altri Stati membri dello Spazio Economico Europeo (SEE), si applica a tutte le società che intrattengono rapporti commerciali con residenti nei paesi dell'UE e verosimilmente anche nei paesi del SEE.
Alla luce di ciò, abbiamo redatto questa breve guida per aiutarti a capire di cosa tratta tale normativa e quali sono le misure da adottare per garantire la tua conformità al regolamento.

Cos'è il GDPR e come si applica alle aziende?

Il sito EUGDPR.org, definisce il GDPR come un regolamento attraverso cui il Parlamento Europeo, il Consiglio dell'Unione Europea e la Commissione Europea intendono rafforzare e rendere più omogenee le normative esistenti sulla protezione dei dati di tutte le persone all'interno dell'Unione Europea.

Il GDPR ha come obiettivo quello "di armonizzare le leggi in materia di riservatezza dei dati in tutta l'Europa, per proteggere e consentire la riservatezza dei dati di tutti i cittadini dell'UE e per ridefinire le modalità di approccio delle organizzazioni per quanto riguarda la riservatezza dei dati." Il regolamento si riferisce quindi a diversi dati personali quali nome, indirizzo, fotografie, indirizzi di posta elettronica, ecc.

Sebbene il GDPR possa apparire come un regolamento completamente nuovo, è possibile che conosciate già il suo predecessore, la direttiva 95/46/CE sulla protezione dei dati personali. Attualmente tutte le aziende e gli enti che trattano dati personali devono rispettare questa direttiva, quindi è probabile che all'interno della vostra organizzazione siano già in atto misure che soddisfano i suoi requisiti, molti dei quali sono simili – ma non necessariamente identici – ai requisiti del GDPR.

Uno dei cambiamenti principali è l'estensione della giurisdizione del GDPR. Il nuovo regolamento si applica a tutte le organizzazioni che trattano dati personali di interessati residenti nell'UE, indipendentemente dall'ubicazione dell'organizzazione stessa. Ciò significa che il GDPR si applica anche al trattamento dei dati personali di persone appartenenti all'UE ad opera di un titolare del trattamento o di un responsabile del trattamento non stabilito all'interno dell'UE, ma offre servizi e beni a residenti dell'UE (indipendentemente dal fatto che vi sia un pagamento correlato) e si occupa del monitoraggio del comportamento di tali interessati all'interno dell'UE.

È fondamentale che tutte le organizzazioni applichino una strategia GDPR – l'inazione non è un'alternativa, in quanto la mancata ottemperanza ai requisiti del GDPR potrà portare a sanzioni fino a 20 milioni di euro o fino al 4% del fatturato mondiale totale annuo, a seconda di quale sia la cifra maggiore fra le due!

Benefici per le aziende e per gli interessati

Sebbene il GDPR possa apparire a molte aziende come un'altra selva normativa in cui districarsi, esistono evidenti benefici derivanti dalla conformità al regolamento.

Prima di tutto, il GDPR spingerà le aziende a migliorare la raccolta e la gestione dei dati, al fine di riunirli in una piattaforma unificata. Il beneficio diretto sarà la possibilità di individuare e accedere più facilmente ai dati che possono contribuire al successo dell'azienda. Un auspicabile effetto a catena sarà una migliore preparazione delle imprese nell'interazione con i propri clienti, per fornire informazioni più pertinenti su prodotti e servizi. Questo renderà anche più facile rispondere alle richieste dei clienti.

In sostanza, questi vantaggiosi cambiamenti organizzativi forniranno anche un "golden record" ai responsabili del trattamento migliorando la loro posizione con gli assicuratori. Procedure di sicurezza più rigide renderanno l'azienda più affidabile agli occhi delle compagnie di assicurazione. Raggiungere la conformità al GDPR segna un passo avanti per molte aziende, fornendo loro un incentivo a intraprendere misure utili, la cui attuazione era stata rimandata o per cui non erano chiare le modalità di approccio.

Legittimi interessi

Oltre alla ben nota dichiarazione di consenso, esistono altre condizioni legali che permettono di trattare i dati personali acquisiti. Fra questi, casi di negoziazione di un contratto fra parti; esigenze di salvaguardia di interessi vitali dell'interessato; oppure in ottemperanza a obblighi di legge. Una condizione meno nota per il trattamento dei dati è quella dei "legittimi interessi" del titolare del trattamento, secondo la quale i dati personali possono essere trattati in circostanze limitate volte a favorire gli interessi legittimi dell'azienda, a condizione che, così facendo, non interferiscano o pregiudichino i diritti dell'interessato o espongano a rischi i dati personali."

QUAL È LA DIFFERENZA FRA UE E SEE?

Stati membri dell'UE:
Austria, Belgio, Bulgaria, Croazia, Cipro, Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, Irlanda, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia, Portogallo, Romania, Slovacchia, Slovenia, Spagna, Svezia, Regno Unito

Stati membri del SEE:
Tutti gli Stati membri dell'UE + Islanda, Lichtenstein e Norvegia

I 6 PRINCIPI DI PROTEZIONE DEI DATI

Per aiutare le organizzazioni a raggiungere la conformità, il GDPR evidenzia sei principi chiave che tutti i titolari del trattamento e i responsabili del trattamento dovranno seguire. Analizzeremo ciascuno di questi principi e spiegheremo cosa comportano per organizzazioni e proprietari di aziende.

1

Liceità, correttezza e trasparenza – Questo principio stabilisce che i dati personali devono essere trattati "in modo lecito, corretto e trasparente nei confronti dell'interessato". Il titolare del trattamento è tenuto a spiegare all'interessato come i suoi dati verranno trattati.

Questo deve essere fatto in modo chiaro, conciso, trasparente e di facile comprensione.
Inoltre, il concetto di correttezza, implica che il trattamento dei dati avviene conformemente a quanto descritto all'interessato. Infine, liceità significa che il trattamento deve rispettare i requisiti descritti nel GDPR [articolo 5, paragrafo 1(a)]: http:// www.privacy-regulation.eu/en/article-5-principles-relating-to-processing-of-personal-data-GDPR.htm.

2

Limitazione della finalità – secondo questo principio i titolari del trattamento e i responsabili del trattamento, possono raccogliere dati personali solo "per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità".

Ciò significa che il trattamento dei dati è limitato alla finalità per cui tali dati sono stati raccolti inizialmente. Il trattamento "per una finalità diversa" o in una fase successiva non è consentito senza ulteriore autorizzazione legale dell'interessato.

3

Minimizzazione dei dati – Possono essere trattati solo i dati personali "adeguati e pertinenti". La loro raccolta deve essere limitata a quanto necessario per il perseguimento delle finalità per cui i dati verranno trattati. Pertanto, i responsabili del trattamento non potranno raccogliere quantità notevoli di dettagli per uso futuro o per creare un profilo dettagliato del cliente a meno che non si renda necessario per finalità legali.

La minimizzazione dei dati deriva dal principio di limitazione della finalità e afferma chiaramente che le aziende devono raccogliere dati sufficienti per raggiungere la loro finalità fin dal principio, ma non più del necessario.

4

Esattezza – Come nel caso del Data Protection Act, predecessore del GDPR, il principio di esattezza è volto al mantenimento di alti standard di qualità dei dati. Questo significa che i dati devono essere esatti e rivisti periodicamente, in modo che siano aggiornati.

5

Limitazione della conservazione – Uno dei principi più importanti contenuti nel GDPR è che i dati personali devono essere "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati".

I proprietari di aziende sono tenuti a controllare e verificare periodicamente i dati in loro possesso. Devono inoltre provvedere alla cancellazione metodica dei dati non più necessari per la finalità per cui erano stati raccolti.

6

Integrità e riservatezza – Questo principio è particolarmente importante per i responsabili del trattamento, e la violazione dello stesso prevede l'applicazione di pesanti sanzioni pecuniarie. Esso afferma che "i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali".

L'applicazione di questo principio ai responsabili del trattamento è uno dei cambiamenti chiave introdotti dal GDPR, a cui i responsabili del trattamento devono prestare particolare attenzione, sulla scia delle importanti violazioni di dati personali e dei rischi sempre maggiori in merito alla sicurezza dei dati.

Questo significa che i titolari del trattamento e i responsabili del trattamento sono tenuti a condurre una valutazione dei rischi e ad adottare una solida politica di sicurezza dei dati, oltre a osservare le rigide disposizioni di segnalazione delle violazioni del GDPR. Questo principio deve essere seguito attentamente e in maniera efficace, dal momento che importanti violazioni di dati personali sono fonte di imbarazzo oltre a comportare costi significativi per le aziende.

GDPR: I MITI DA SFATARE

Nei mesi e negli anni precedenti all'attuazione del GDPR sono circolate molte speculazioni in merito alle sue implicazioni. Questo ha portato alla nascita di non pochi miti su cosa il GDPR significhi o meno, causando confusione e preoccupazione. In questa sezione affronteremo alcuni dei principali luoghi comuni sul GDPR con l'obiettivo di portare un po' di necessaria chiarezza.

#1: Il GDPR è solo un problema informatico

Il nostro verdetto: FALSO

Poiché la questione si è concentrata sulla sicurezza dei dati e sulla difesa da attacchi ai danni dei sistemi informatici delle aziende, molti ritengono che sia responsabilità del reparto informatico garantire la conformità al GDPR.

In realtà il GDPR riguarda molti più aspetti. Se per soddisfare i requisiti del Data Protection Act del 1998, un'azienda ha investito in sistemi per la protezione dei dati, questi costituiscono una buona base per la conformità al GDPR. Tuttavia, le procedure e le politiche interne dovranno in ogni caso essere valutate e aggiornate per dimostrarne la conformità. L'attenzione dovrebbe essere posta sulla valutazione globale del rischio, sul miglioramento degli standard di protezione dei dati e su efficaci procedure applicabili alla notifica delle violazioni di dati e di perdita di dati.
Sebbene sicurezza e integrità fisica rimangano una priorità del GDPR, nuovi concetti come il "diritto all'oblio" e il "diritto alla portabilità dei dati" dovranno essere tenuti in considerazione da tutti i settori dell'azienda.

#2: L'unico requisito obbligatorio per il trattamento dei dati personali è il consenso

Il nostro verdetto: FALSO

Affinché una società possa archiviare e trattare le informazioni personali di una persona, è necessaria una base legale prima di poter procedere con qualsiasi forma di trattamento dei dati. Il consenso è una di queste basi, ma non l'unica. Il GDPR alza l'asticella in termini di cosa è considerato "consenso" al trattamento dei dati. Le persone dovranno esprimere il consenso selezionando un'apposita casella, mentre le organizzazioni dovranno essere in grado di dimostrare come e quando l'interessato ha prestato questo consenso.

È possibile impostare dei preference centre (noti anche come privacy dashboard) che consentono di avere "scelta e controllo continuativi" sulle modalità in cui viene espresso il proprio consenso. In questo modo, quando una persona desidera revocare il consenso al trattamento dei propri dati, tale revoca dovrebbe essere attuabile con la stessa modalità utilizzata per l'autorizzazione.

#3: Non segnalare in tempo una violazione può portare a pesanti sanzioni

Il nostro verdetto: VERO

Le autorità di controllo di ogni stato avranno il diritto di infliggere sanzioni alle imprese che negano la violazione di dati e non effettuano la notifica di tale violazione entro 72 ore. Le sanzioni possono essere evitate nella misura in cui le organizzazioni sono aperte, oneste e comunicano senza ingiustificato ritardo. Tutto ciò va di pari passo con i principi base di trasparenza del GDPR.
Tutto si traduce nell'adozione delle migliori prassi e in una condotta il più onesta possibile qualora le cose vadano male. L'autorità fornirà supporto e consulenza per aiutare le aziende a stare dalla parte giusta della legge ed evitare sanzioni.

#4: Tutte le organizzazioni dovranno nominare un responsabile della protezione dei dati

Il nostro verdetto: FALSO

Il GDPR non richiede la nomina obbligatoria di un responsabile della protezione dei dati, ma è consigliabile che le organizzazioni più grandi prevedano questo ruolo. Recenti sondaggi condotti nel Regno Unito, dimostrano che il 70% delle aziende con oltre 100 dipendenti hanno già nominato un responsabile della protezione dei dati, il che è un grande passo in avanti verso attività di trattamento dei dati coerenti e lecite.

#5: Tutte le violazioni dei dati dovranno essere notificate alle autorità

Il nostro verdetto: FALSO

Qualora una violazione dei dati possa danneggiare i diritti e le libertà delle persone, è obbligatorio riferire tale violazione alle autorità nazionali di protezione dei dati. La mancata notifica entro 72 ore prevede pesanti sanzioni. Tuttavia, se è improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone, le imprese non sono tenute a notificarla.

La difficoltà qui sta nello stabilire la soglia oltre la quale un incidente sia da notificare o meno alle autorità. Un approccio pragmatico in caso di incertezza consiste nel segnalare tutte le violazioni di dati, rivolgendosi alle autorità per una consulenza sulla migliore linea d'azione da adottare.

Prodotti conformi al GDPR

L'imminente arrivo del GDPR ha spinto molte imprese a tentare di guadagnarsi un vantaggio competitivo promettendo prodotti e servizi conformi al GDPR. In realtà, pochissime organizzazioni sono in grado di fornire consulenza ad altre aziende, e le autorità stanno mettendo in guardia le persone affinché prestino la massima attenzione nel momento in cui decidono di affidare la sicurezza dei propri dati a imprese che sostengono di essere conformi al GDPR.

Sebbene sia azzardato affermare che è possibile raggiungere la conformità seguendo procedure "preconfezionate", è anche vero che alcuni prodotti possono essere d'aiuto alle organizzazioni ai fini della conformità, per esempio la cifratura dei dati gestiti o l'automazione dei processi aziendali per il trattamento dei dati. Ecco alcuni metodi sicuri per scegliere le soluzioni più adatte supportare le attività di implementazione delle disposizioni del GDPR, e la buona notizia è che queste soluzioni sono relativamente facili da applicare.

Il primo passo, e il più importante, è quello di mettere in atto una procedura di valutazione dei dati chiara e affidabile. Per farlo, le organizzazioni dovrebbero scegliere di collaborare con un partner riconosciuto, che li aiuti a valutare i metodi che utilizzano per la gestione di documenti e dati all'interno della propria azienda. Qualora vengano riscontrate delle carenze, un partner esperto e ben informato sarà in grado di consigliare strumenti hardware e software affinché le procedure siano conformi con le nuove regole.

Fra questi, per esempio, il miglioramento della sicurezza dei dati attraverso la crittografia end-to-end con il supporto del protocollo SSL e IPSec, l'utilizzo di sistemi di sovrascrittura dei dati e la protezione del disco rigido dei dispositivi di stampa. Un buon partner per il trattamento dei dati sarà anche in grado di gestire i dati originali richiesti o non richiesti provenienti dalle innumerevoli applicazioni back end e dai sistemi ERP aziendali.

Conservare tutti i documenti in un archivio centrale che possa essere controllato e con accesso limitato, offrirà un livello di sicurezza maggiore, dal momento che l'accesso alle informazioni sensibili sarà impedito al personale aziendale non autorizzato.

Il supporto nella gestione dei dati può anche aiutare a uniformare il processo di raccolta di tutti i dati o documenti che entrano nell'azienda, in modo che tutti i dati personali vengano gestiti in modo coerente, classificati, indicizzati e archiviati per facilitarne e velocizzarne il recupero.

Ciò è importante perché il GDPR sancisce il "diritto di accesso" e il "diritto all'oblio", secondo i quali gli interessati possono richiedere le copie di tutti i propri dati personali, o la cancellazione di tutti i dati vecchi o non essenziali. I sistemi di gestione dei dati rendono semplice e automatico il processo di cancellazione dei dati quando questi non servono più, oppure il recupero degli stessi in caso di richiesta del cliente.

IN SINTESI

La sicurezza dei dati e il diritto delle persone di controllare l'utilizzo dei propri dati personali sono da tempo una materia rilevante per l'Unione Europea. Ci sono state importanti e ripetute violazioni di dati che hanno reso chiara la necessità di una migliore gestione e sicurezza nelle PMI così come nelle imprese multinazionali. Il GDPR è impostato per alzare gli standard e spingere i titolari del trattamento e i responsabili del trattamento a migliorare i propri sistemi e procedure. Nessuno può permettersi di rimanere indietro!

GLOSSARIO

Responsabile del trattamento	In riferimento ai dati personali, identifica a qualsiasi persona (diversa da un dipendente del titolare del trattamento) che tratta dati personali per conto del titolare del trattamento.
Titolare del trattamento	La persona che (singolarmente o insieme ad altri) determina le finalità e le modalità con le quali i dati personali sono o saranno trattati.
Trattamento dei dati	Si riferisce alla raccolta, registrazione, conservazione, o a qualsiasi operazione o insieme di operazioni applicate a informazioni o dati, incluso - a) l'organizzazione, l'adattamento o la modifica delle informazioni o dei dati, b) l'estrazione, la consultazione o l'uso delle informazioni o dei dati, c) la comunicazione delle informazioni o dei dati mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, oppure d) il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione delle informazioni o dei dati
SSL	Il **Secure Sockets Layer** è un protocollo volto a rendere sicura la trasmissione di informazioni dal client al server su cui vengono caricati i dati.
IPsec	L'**Internet Protocol Security** è una serie di protocolli di sicurezza a livello di comunicazione di rete.

Link utili

Informazioni generali:
http://www.eugdpr.org

Il testo completo del GDPR:
http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679