solarwinds msp

E-BOOK

GDPR 101

Informazioni che gli MSP dovrebbero conoscere

A seguito della decisione di implementare il regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation) a maggio 2018, consulenti IT e provider di servizi gestiti (MSP) si chiedono quali saranno le conseguenze sul loro lavoro. In molti casi, la stampa di settore ha discusso di questa nuova legge con un misto fra panico e costernazione. La decisione è sicuramente sensata, poiché la nuova legge impone alle organizzazioni di rafforzare le proprie misure di sicurezza, pena il pagamento di multe potenzialmente molto salate.

In questo e-book, tratteremo alcuni aspetti chiave del GDPR e spiegheremo come influirà sul lavoro degli MSP. Discuteremo di alcune delle sfide che si imporranno e, speriamo, attenueremo alcune delle paure che gli MSP potrebbero avere mentre tentano di individuare l'approccio da adottare nel proprio lavoro.

Informazioni chiave sul GDPR[1]:

1. Multe più salate
2. Consenso chiaro ed esplicito al trattamento dei dati per finalità di marketing
3. Notifica per violazione dei dati entro 72 ore per i titolari del trattamento dei dati
4. Copertura geografica estesa
5. Responsabilità condivisa
6. Diritto di cancellazione, uno dei diritti estesi per i soggetti interessati
7. Legislazione semplificata sui dati
8. Sicurezza del trasferimento dei dati
9. Applicazione del GDPR
10. Sanzioni universali

1. Multe più salate

Sebbene il cosiddetto fattore FUD (Fear, Uncertainty, and Doubt, cioè paura, incertezza e dubbio) sia stato dichiarato molto elevato, gli MSP potranno ridurre moltissimi problemi semplicemente prendendo molto seriamente questo nuovo regolamento.

Nel post pubblicato su un blog il 15 settembre 2017, Elizabeth Denham, commissario per l'informazione degli uffici del Regno Unito dell'Information Commissionaire (ICO) suggerisce che tale fattore FUD sia piuttosto "allarmistico". Il commissario prosegue dichiarando: "L'impegno dell'ICO di guidare, consigliare e formare le organizzazioni al rispetto del nuovo regolamento non cambierà con l'entrata in vigore del GDPR. Abbiamo sempre preferito la carota al bastone."[2]

Denham cita alcuni fatti per dimostrare il suo punto di vista e scrive: "L'imposizione di sanzioni è sempre stata, e continuerà a essere, un'estrema ratio. Nell'ultimo anno (2016/2017), abbiamo concluso 17.300 casi, 16 dei quali hanno visto l'erogazione di multe per le organizzazioni coinvolte, ma non abbiamo ancora messo in campo tutte le nostre risorse. Dichiarare che col GDPR aumenteranno le sanzioni rispetto ai casi valutati in base al Data Protection Act non ha alcun senso".[3] In altre parole, niente panico: è sufficiente prendere molto seriamente il nuovo regolamento e, proprio come suggeriscono le best practice, prepararsi a seguire le linee guida al meglio delle proprie possibilità.

2. Consenso chiaro ed esplicito al trattamento dei dati per finalità di marketing

Molti MSP avvertiranno l'impatto del GDPR nelle iniziative di commercializzazione i propri servizi a nuovi clienti. In base al GDPR, infatti, le aziende devono ottenere il consenso per inviare messaggi con finalità di marketing (qualora non possano trattare i dati sulla base giuridica di un interesse legittimo).

Le cose si complicano quando si tratta di comunicazioni B2B. Il nuovo regolamento, infatti, permette alle aziende di inviare comunicazioni direttamente ad altre imprese senza il consenso esplicito dei destinatari. Questo richiede una certa dovuta diligenza da parte del mittente che deve accertarsi che il destinatario sia effettivamente un'azienda. In generale, le regole per il marketing destinato alle aziende non sono così rigorose.

Per saperne di più sulle informazioni di marketing per cui vige la base giuridica del consenso esplicito per il trattamento dei dati, consigliamo di leggere la checklist dell'ICO reperibile qui (in lingua inglese): https://ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf.

In base al GDPR, le aziende, per poter inviare messaggi con finalità di marketing, devono ottenere l'esplicito consenso degli individui.

3. Notifica per violazione dei dati entro 72 ore per i titolari del trattamento dei dati

Il termine di 72 ore per segnalare una violazione dei dati è l'aspetto che maggiormente desta preoccupazioni. È importante per i titolari del trattamento dei dati conformarsi a tale regola, ma anche conoscerne alcune sfumature. Ecco la differenza fra titolari e responsabili del trattamento dei dati: i titolari del trattamento dei dati sono persone fisiche o giuridiche, autorità pubbliche, servizi o altri organismi che determinano le finalità, le condizioni e i mezzi del trattamento dei dati personali, mentre i responsabili del trattamento dei dati sono i soggetti giuridici che trattano i dati personali per conto del titolare del trattamento.[4]

Nel GDPR è presente un provvedimento piuttosto vago (GDPR REF) in merito alla notifica che lascia fin troppo spazio all'interpretazione. In poche parole, gli incidenti vanno segnalati a un'autorità di supervisione in base ad alcuni fattori di rischio. L'ICO suggerisce:

> *Le linee guida paneuropee aiuteranno le organizzazioni a definire le soglie di segnalazione, ma l'approccio ottimale sarà quello di iniziare a esaminare le tipologie di incidenti con cui le organizzazioni hanno a che fare e stabilire quali casi rappresentano incidenti seri nel contesto dei dati e dei clienti.*[5]

In assenza di linee guida specifiche, l'ICO suggerisce che siano le organizzazioni a stabilire se le violazioni dei dati hanno un impatto negativo significativo sulle persone, ad esempio "discriminazioni, danni alla reputazione, perdita di riservatezza, perdite finanziarie o altri svantaggi economici o sociali significativi".[6]

Ugualmente ambigui sono gli aspetti da segnalare entro il termine di 72 ore. In base al GDPR, laddove l'organizzazione non disponga di tutti i dettagli sulla violazione, essa può produrre la documentazione necessaria anche dopo il termine previsto. Anche laddove l'autorità di supervisione del GDPR voglia conoscere il potenziale ambito e le cause della violazione dei dati, le misure di contenimento che si intende adottare e il piano per risolvere il problema, tali dati potrebbero non essere disponibili. In questo caso, sembra sia possibile produrre una documentazione dettagliata aggiuntiva anche oltre il termine di 72 ore.

È importante per i titolari del trattamento dei dati conformarsi a tale regola, ma anche conoscerne alcune sfumature...

4. Copertura geografica estesa

Per gli MSP che si rivolgono ad aziende dell'Unione Europea e del Regno Unito dall'estero (ad esempio Stati Uniti o Canada), questa parte del regolamento potrebbe causare qualche perplessità.

Si tratta di un tentativo, non diverso dall'estensione delle leggi statunitensi al di fuori della giurisdizione degli Stati Uniti, di applicare i requisiti del GDPR a qualsiasi impresa che abbia clienti residenti in UE o nel Regno Unito. In teoria, l'idea di estendere la severità e le best practice della conformità al GDPR ai dati dei cittadini dell'Unione Europea e del Regno Unito, a prescindere dalla sede di archiviazione, è molto sensata, tuttavia, sarà interessante vedere come e in quali circostanze le autorità applicheranno questa parte del regolamento. In ogni caso, qualsiasi impresa esterna ai confini dell'Unione Europea dovrà prendere questo regolamento molto seriamente e fare tutto il possibile per prepararsi all'entrata in vigore della legge.

Qualsiasi impresa esterna ai confini dell'Unione Europea dovrà prendere questo regolamento molto seriamente e fare tutto il possibile per prepararsi all'entrata in vigore della legge.

5. Responsabilità condivisa

Titolari o responsabili del trattamento dei dati? Molte leggi in UE e nel Regno Unito tendevano a dare maggiore responsabilità ai titolari del trattamento rispetto ai responsabili, ma il GDPR ha invertito questa tendenza. Sia titolari sia responsabili del trattamento, infatti, ora condividono le medesime responsabilità rispetto alla tutela delle informazioni di identificazione personale.

Per gli MSP, proprio come per la maggior parte delle imprese, questo approccio ha alcune sfumature. La realtà è che, se la responsabilità della tutela è condivisa equamente tra titolari e responsabili del trattamento dei dati, perdere troppo tempo a determinare i ruoli e l'effettiva responsabilità di MSP e parti terze può essere inutile. A prescindere dal ruolo dell'impresa, è responsabilità degli MSP prepararsi all'entrata in vigore del GDPR. Gli MSP, pertanto, dovranno impegnarsi a salvaguardare le informazioni di tutti i clienti (nonché le informazioni di identificazione personale dei dipendenti).

6. Diritto di cancellazione, uno dei diritti estesi per i soggetti interessati

Sebbene il GDPR preveda che ogni individuo possa richiedere la rimozione dei propri dati archiviati presso un'azienda (diritto all'oblio o di cancellazione), per le organizzazioni questa possibilità è difficile da garantire. Poiché tale diritto non è esercitabile in caso di trasferimento dei dati personali per determinate basi giuridiche, diventa difficile stabilire le circostanze in cui concedere il diritto di cancellazione. Inoltre, è necessario considerare eventuali limitazioni tecniche dei sistemi.

In molti paesi si richiede la conservazione della documentazione aziendale e di alcune categorie di dati personali. Questo aspetto potrebbe generare conflitti, laddove il diritto all'oblio contraddica il diritto legale di conservare o di fornire accesso alla documentazione. Tale conflitto principalmente si palesa nei settori sanitario, legale e finanziario. Prima di eliminare in modo permanente documenti aziendali per conto dei clienti, al fine di tutelarsi, gli MSP devono rivolgersi a un legale in merito alle leggi in vigore e alla conformità al GDPR.

7. Legislazione semplificata sui dati

L'obiettivo globale del GDPR è quello di consolidare la miriade di leggi in materia di tutela dei dati in vigore nei singoli paesi dell'UE in uno standard universalmente riconosciuto e applicato in tutta l'Unione. Sebbene il GDPR raggiunga da un lato questo obiettivo, sono presenti leggi approvate nei singoli paesi che potrebbero includere requisiti che vanno oltre l'ambito di applicazione del GDPR. La legislazione tedesca, ad esempio, prevede che le informazioni di identificazione personale dei cittadini tedeschi restino in Germania.

L'obiettivo globale del GDPR è quello di consolidare la miriade di leggi in materia di tutela dei dati in vigore nei singoli paesi dell'UE in uno standard universalmente riconosciuto e applicato in tutta l'Unione.

Altre leggi dell'UE prevedono restrizioni geografiche nell'ambito dell'archiviazione o della trasmissione dei dati fra paesi, in genere per il settore finanziario e sanitario. Per gli MSP che erogano servizi a clienti residenti in diversi paesi dell'Unione Europea, è importante garantire che le soluzioni di backup o altri strumenti disponibili non violino i regolamenti circa la posizione geografica.

8. Sicurezza del trasferimento dei dati

Analogamente ai punti 4 e 7, questo aspetto presenta alcune soprattutto principalmente per le aziende globali che trasmettono enormi quantità di dati da e verso UE e Regno Unito. Per gli MSP è fondamentale verificare che strumenti e fornitori di terze parti siano conformi ai requisiti in materia di privacy e di sicurezza previsti dal GDPR.

Per gli MSP è fondamentale verificare che strumenti e fornitori di terze parti siano conformi ai requisiti in materia di privacy e di sicurezza previsti dal GDPR.

Gli MSP che operano nell'area geografica dell'UE e del Regno Unito dovranno garantire che il trasferimento dei dati sia effettuato in un regime di privacy dei dati, ad esempio quello previsto dallo Scudo UE-USA per la privacy o da norme aziendali vincolanti. A prescindere dal metodo scelto per il trasferimento dei dati, le misure di tutela della privacy devono essere conformi ai requisiti del GDPR. Per i dati a riposo in un paese esterno all'area UE/Regno Unito, i diritti di privacy dovranno comunque essere conformi ai requisiti imposti dal GDPR. Ad esempio, un MSP che si rivolge a uno studio legale internazionale potrebbe dover implementare un servizio sicuro specifico per far sì che i dati siano conformi ai requisiti di tutela dei dati previsti dal GDPR.

9. Applicazione del GDPR

La creazione di un regolamento paneuropeo in materia di tutela dei dati come il GDPR che andrà rispettato a livello universale richiede un piano di applicazione. Per le fasi iniziali dell'applicazione del GDPR, sono previste alcune problematiche poiché alcuni paesi sono un passo avanti nell'ambito delle verifiche di dovuta diligenza per la sicurezza informatica.

Ad esempio, lo schema Cyber Essentials del Regno Unito è un programma governativo che prevede alcune best practice per la tutela dei dati. Non tutti i paesi di UE e Regno Unito hanno implementato un programma come questo. Pertanto, sarà difficile applicare uno standard in tutti i paesi che non ne hanno uno.

Lo schema Cyber Essentials del Regno Unito è un programma governativo che prevede alcune best practice per la tutela dei dati. Non tutti i paesi di UE e Regno Unito hanno implementato un programma come questo.

Gli MSP che desiderino attuare delle regole di base per i servizi di sicurezza e la conformità al GDPR dovranno individuare un framework di sicurezza IT di riferimento. Gli standard internazionali come l'ISO 27001 potrebbero consentire di dimostrare la conformità dei servizi erogati alle best practice. Se le organizzazioni sono in grado di dimostrare l'applicazione di opportune best practice potrebbero riuscire a ridurre la drasticità delle pene pecuniarie per violazione dei dati.

10. Sanzioni universali

Probabilmente la sezione del GDPR con maggiore impatto è quella che riguarda il tentativo di applicare universalmente pene deterrenti per le violazioni del GDPR. Come precedentemente menzionato al punto 5, la responsabilità della tutela dei dati è distribuita equamente tra il titolare e il responsabile del trattamento dei dati, pertanto pare che il GDPR sia stato implementato per garantire in modo severo la tutela dei dati in UE e Regno Unito. La legge impone alle organizzazioni di garantire la presenza di un'opportuna tutela in base al GDPR, di proteggere i dati di identificazione personale e di impiegarli secondo la legge e con il consenso esplicito dei soggetti interessati. A prescindere dagli accordi in vigore tra clienti e imprese, il GDPR resta in vigore.

A prescindere dagli accordi in vigore tra clienti e imprese, il GDPR resta in vigore.

Per gli MSP questo aspetto comporta conseguenze positive e negative. Tra le conseguenze positive, MSP e loro clienti si trovano sulla stessa barca, pertanto devono collaborare fianco a fianco per proteggere i dati di identificazione personale. Tra le conseguenze negative, gli MSP devono garantire e documentare in buona fede misure atte alla tutela dei dati per i servizi erogati. In breve, né le imprese né gli MSP potranno eludere in alcun modo le proprie responsabilità nell'applicazione del GDPR.

La maggioranza degli MSP è in buona fede e collabora con i propri clienti. Sebbene il GDPR modifichi alcuni approcci degli MSP e ponga alcune problematiche per l'erogazione dei servizi, gli MSP che operano all'interno di UE e Regno Unito saranno già avvezzi ad agire sulla base di una sorta di legge atta a tutelare i dati. Il GDPR non deve pertanto causare panico: come menzionato in precedenza, le autorità dell'UE hanno dichiarato che il loro intento è tenere presenti le circostanze specifiche delle organizzazioni. È opportuno che gli MSP si facciano consigliare in ambito normativo da un legale di fiducia del proprio paese di residenza per garantire che servizi, fornitori e best practice adottati siano allineati all'intento del GDPR di tutelare le informazioni di identificazione personale in UE e Regno Unito.

1. "Home Page of GDPR." http://www.eugdpr.org/eugdpr.org.html Trunomi (consultato a settembre 2017).

2. "GDPR – Sorting Fact from Fiction," Elizabeth Denham. https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/ (consultato a settembre 2017).

3. "GDPR – Sorting Fact from Fiction," Elizabeth Denham. https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/ (consultato a settembre 2017).

4. "Home Page of GDPR." http://www.eugdpr.org/eugdpr.org.html Trunomi (consultato a settembre 2017).

5. "GDPR – Sorting Fact from Fiction," Elizabeth Denham. https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/ (consultato a settembre 2017).

6. Breach Notification, Information Commissioner's Office. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/ (consultato a settembre 2017)