METHA GROUP®

IT Around Your Business

GDPR: Regolamento Generale per la Protezione dei Dati


» SECURITY «

Questa guida di Metha Group presenta il Regolamento Generale sulla Protezione dei Dati (GDPR), le implicazioni e le potenziali sfide che le organizzazioni devono affrontare per diventare conformi e il ruolo che i Partner possono svolgere nel supportarle in questo percorso verso la conformità.

Contesto del GDPR

Nel gennaio del 2012, la Commissione Europea ha presentato la Riforma dell'UE in materia di protezione dei dati, affinché l'Europa rimanesse al passo con le evoluzioni dell'era digitale. Secondo la Commissione, oltre il 90% degli europei afferma di volere gli stessi diritti in materia di protezione dei dati in tutta l'UE, indipendentemente da dove vengono trattati. Il 15 dicembre 2015, il Parlamento Europeo, il Consiglio e la Commissione hanno raggiunto un accordo sulla nuova normativa in materia di sicurezza, istituendo un quadro moderno e armonizzato per la protezione dei dati in tutta l'UE. Il GDPR (Regolamento Generale sulla Protezione dei Dati) è il frutto del lavoro dell'Unione Europea per allineare la normativa in materia di protezione dei dati alle modalità con cui essi vengono ora utilizzati. Il GDPR prevede che tutte le aziende dovranno essere conformi entro il 25 maggio 2018 e andrà a sostituire il Data Protection Act del 1998 e altri regolamenti in materia di data protection.

La situazione attuale

In questo momento, i dati personali trattati all'interno dell'Unione Europea sono disciplinati dalla Direttiva europea del 1995 (95/46/CE) sulla protezione degli individui in materia di trattamento degli stessi e sulla libera circolazione di essi (Direttiva). Questo riguarda i dati dei cittadini dell'UE e le modalità con cui essi vengono elaborati, utilizzati o scambiati, soprattutto dalle aziende.

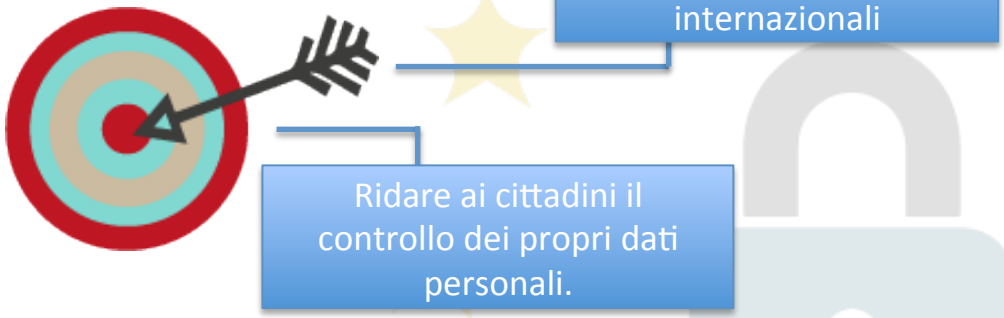
25/05/2018

A meno di 12 mesi dall'entrata in vigore del GDPR, molte aziende non sono ancora pronte per le modifiche necessarie da implementare per essere conformi.

Per le organizzazioni internazionali, la situazione attuale potrebbe trasformarsi in una vera e propria sfida in quanto dovranno impegnarsi con i regolatori in ogni Stato membro, ognuno dei quali prevede requisiti legali diversi. In effetti, qualsiasi informazione che potrebbe essere utilizzata per identificare un individuo rappresenta un dato personale. Ad esempio, un elenco di nomi e indirizzi di clienti è considerato un elenco di dati personali, proprio come un database con gli indirizzi e-mail dei clienti. Inoltre, anche dati incompleti sugli individui possono comunque essere considerati tali.

Obiettivi del GDPR

L'obiettivo del GDPR è aumentare gli obblighi e i vincoli in capo alle aziende che trattano dati personali.



Questo dovrebbe ridurre il costo a carico delle aziende per ottenere la conformità, applicando in tutti gli Stati membri gli stessi requisiti di conformità previsti nel GDPR. Tuttavia, le sanzioni in caso di non conformità costituiscono un notevole rischio per le aziende, con multe per infrazioni fino a 20 M€ o pari al 4% del fatturato annuo mondiale del gruppo.

Anche le imprese al di fuori dell'UE possono essere impattate direttamente dal GDPR. Qualsiasi azienda che offre beni o servizi, che fa profilazione oppure che si rivolge, in qualsiasi modo, a soggetti titolari di dati all'interno dell'UE, dovrà rispettare il GDPR. Inoltre, le organizzazioni internazionali che trasferiscono i dati da un Paese all'altro possono ora indicare e identificare una struttura principale e l'autorità di vigilanza in quel Paese sarà il loro principale contatto a livello normativo.

Le responsabilità derivanti dal GDPR

I nuovi regolamenti daranno maggiori responsabilità ai "controller", ossia i responsabili del trattamento dei dati e ai "processor", ossia gli incaricati del trattamento dei dati, per garantire che le imprese rispettino il GDPR. Tuttavia, è il "controller" il vero responsabile dei dati personali all'interno della supply chain.

Controller

L'entità (azienda, organizzazione, autorità, agenzia) che determina le finalità, le condizioni e gli strumenti utilizzati per il trattamento dei dati personali e spiega come e perché essi vengono elaborati.
Un controller dovrà garantire che tutti gli obblighi contrattuali definiti con un "processor" siano conformi al GDPR.

Processor

Agisce per conto del "controller", elaborando i dati nel modo indicato dal controller. Mentre egli determina il "come" e il "perché", è il "processor" che sarà tenuto a mantenere i registri dei dati personali in proprio possesso e le modalità di trattamento di quegli stessi dati.

Un processor avrà maggiori responsabilità legali nel caso in cui si rende responsabile di una violazione. Tali obblighi e responsabilità in capo al processor rappresentano una nuova disposizione all'interno del GDPR.

Principali considerazioni sul GDPR

Il concetto di protezione dei big data "by design" e "by default", sarà parte integrante di tutti i progetti che riguardano i dati personali. Qualsiasi progetto dovrà essere avviato andando, in primis, a promuovere i principi della privacy e della protezione dei dati, anziché basarsi semplicemente su un approccio a posteriori, o addirittura ignorando totalmente la questione.

Crittografia:
La crittografia e altre misure di sicurezza sono definite come standard di protezione dei dati e si prevede che le organizzazioni utilizzino la crittografia per proteggere i dati personali.

Audit di conformità:
Le organizzazioni dovranno realizzare degli audit in alcuni dipartimenti e/o uffici particolari o in maniera trasversale in tutta l'azienda.

Trasparenza e consenso:
Le comunicazioni destinate e relative agli individui dovranno essere trasparenti. Esistono diverse basi per il trattamento dei dati personali, e il consenso è una di queste.

Dati disciplinati
Le definizioni di "Dati Personali" e "Dati Sensibili" sono state ampliate. Quest'ultima, per esempio, include ora i dati genetici e biometrici.

Comunicazione di violazione dei dati personali:
Gli obblighi di notifica (alle autorità di vigilanza e agli individui) scattano in caso di distruzione, perdita, alterazione, divulgazione non autorizzata o accesso a dati personali che avvenga in maniera involontaria o illegale. Le suddette notifiche dovranno essere effettuate entro 72 ore dal momento in cui ne si è venuti a conoscenza, sia all'autorità competente che agli individui, in caso di rischio per i loro dati.

Autorità di vigilanza:
La vigilanza normativa sulla protezione dei dati cambierà in maniera significativa, anche attraverso l'introduzione di un'autorità di controllo per alcune organizzazioni che lavorano in Paesi diversi all'interno dell'UE.

Pseudonimizzazione:
È un principio secondo il quale l'individuo non può essere identificato direttamente tramite un singolo dato, ma è solo l'aggregazione di dati diversi che può portare alla sua identificazione.

Maggiori diritti:
Ai soggetti titolari di dati sono attribuiti diritti sostanziali, tra cui il diritto all'oblio, il diritto alla portabilità dei dati e il diritto di opporsi al processo decisionale automatizzato.

Protezione dei dati by design e responsabilità:
Il controller titolare del trattamento dei dati avrà la responsabilità dei dati all'interno della propria supply chain. È responsabilità di tutti i controller e di tutti i processor dimostrare il rispetto della normativa sul trattamento dei dati personali e sulla privacy in vigore nei Paesi membri dell'Unione Europea.

Minori e consenso:
È necessario un consenso genitoriale verificabile per l'utilizzo dei dati personali di un minore nell'ambito di servizi online e solo per minori al di sotto dei 16 anni di età. Questo è uno degli atti delegati che devono essere confermati per l'utilizzo dei dati personali di un minore.

Implicazioni del GDPR

Le implicazioni del GDPR potrebbero diventare una preoccupazione nel momento in cui si opera all'interno dell'UE e si debba gestire dati /informazioni relative a singoli individui. Il GDPR avrà indubbiamente un impatto sull'attività di qualsiasi azienda che possiede o tratta dati sui cittadini dell'Unione Europea, indipendentemente dal luogo in cui si trova la sede legale o se, nell'ambito della propria attività, commercializza o tratta tali dati all'interno dell'Unione oppure no.

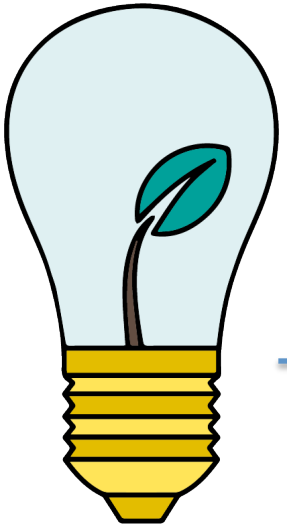
Secondo la nuova normativa, un funzionario responsabile della protezione dei dati ("Data Protection Officer") deve informare direttamente l'amministratore delegato o la persona più senior della propria azienda: è quindi fondamentale che il senior management svolga un ruolo attivo nell'implementazione del GDPR. Infine, coloro che avranno una responsabilità strategica e operativa saranno incaricati di mitigare i rischi del GDPR, considerando sia le opportunità che le minacce per l'attività dell'azienda.

Punti chiave da considerare per essere conformi al GDPR

- Le organizzazioni devono adottare misure tecniche e organizzative per dimostrare la loro conformità con il GDPR, il che significa che dovranno sviluppare nuove policy, nuovi controlli e nuove procedure.
- Le aziende sono tenute ad adottare soluzioni all'avanguardia nella progettazione e nell'esecuzione delle loro responsabilità in materia di protezione dei dati e nell'implementazione delle relative misure di sicurezza.
- Per essere conformi al GDPR, potrebbe essere necessario allocare un determinato budget e un certo numero di risorse.
- Le organizzazioni dovranno garantire che i loro sistemi di sicurezza assicurino la conformità e dovranno rivedere le loro infrastrutture e servizi.
- La protezione dei dati sta diventando un problema che riguarda direttamente il Consiglio di Amministrazione.
- Le valutazioni dell'impatto sulla protezione dei dati DEVONO essere condotte quando si verificano rischi specifici per i diritti e le libertà dei soggetti interessati.
- Esistono implicazioni legate a costi di assicurazione potenzialmente elevati in base al livello di sicurezza implementato. Il ROI della sicurezza sarà più visibile (il calcolo dei rischi effettuato dalle compagnie di assicurazione sarà più efficace).
- Sarà necessario modificare i contratti in essere, con un impatto per i Partner.
- Possibile perdita di attività nei confronti di competitor conformi.
- In caso di violazione, le sanzioni potranno arrivare fino a 20 milioni di euro o al 4% del fatturato annuo di gruppo.
- Le violazioni avranno un impatto sulla fiducia dei clienti, con un rischio di calo delle attività e un aumento dei relativi costi per porvi rimedio.
- I risarcimenti potrebbero essere un problema, con i controller autorizzati a trattenere e recuperare l'eventuale pagamento di risarcimenti se un processor all'interno della supply chain è ritenuto non conforme ed è stato la causa di tale violazione.
- In caso di violazione della sicurezza, questa dovrà essere segnalata all'autorità di vigilanza e agli individui interessati entro 72 ore dal momento in cui ne si è venuti a conoscenza.

Nuove opportunità per i partner di canale

Le nuove normative dell'UE, in materia di protezione dei dati, rappresentano una grande opportunità per i Partner che si occupano di consulenza, sicurezza, storage e tecnologie. La severità delle sanzioni, accompagnata dai sostanziali cambiamenti legati all'ambito di applicazione, spingeranno le aziende a modificare radicalmente le loro pratiche legate alla protezione dei dati, cercando il supporto di partner e di nuove tecnologie per ottenere la conformità.

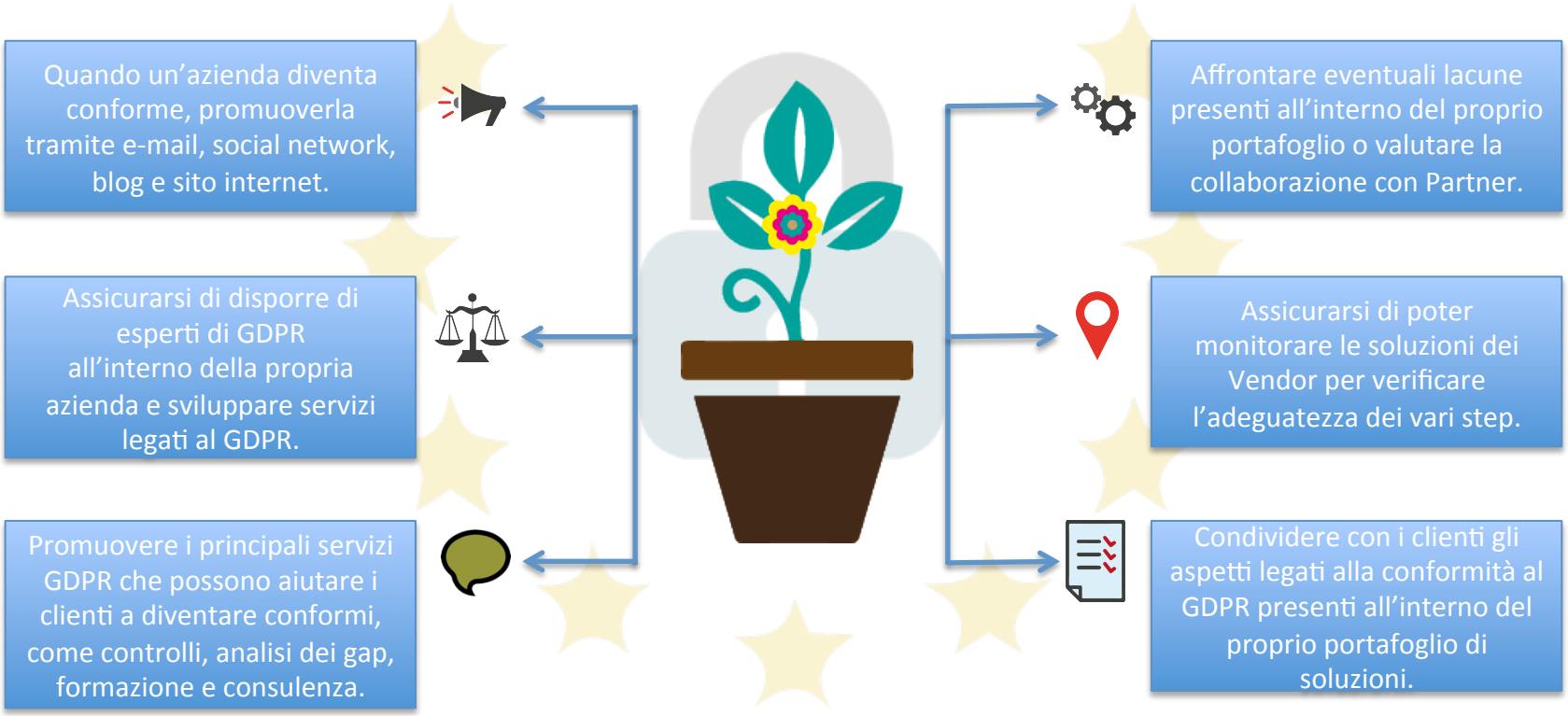


- Comunicazione della propria conformità. Ottenere più business rispetto ad aziende concorrenti non conformi.
- Costi assicurativi ridotti in caso di conformità. Negoziazione di contratti migliori con i fornitori (ai danni di fornitori non conformi).
- Obiezioni di non conformità da parte di clienti esistenti passati. Perdita di clienti /prospect rispetto a concorrenti conformi.
- Sanzioni normative (20 milioni di euro o il 4% del fatturato annuo di gruppo)
  Premi assicurativi più alti in caso di non conformità
  Richieste di risarcimento dei clienti.

In generale, tutti i tipi di Partner dovranno **essere esperti**, fornendo ai clienti consulenza, formazione, soluzioni e instaurando, di conseguenza, rapporti di partnership commerciale a lungo termine basati sulla fiducia. Inoltre, se questi Partner trattano dati personali per conto dei loro clienti, dovranno tassativamente rispettare il GDPR oppure il cliente non sarà legalmente autorizzato a nominarli.

Capitalizzare sul GDPR

L'impatto del GDPR potrà variare a seconda dell'organizzazione del cliente. I seguenti punti dovrebbero essere considerati all'interno della (nuova) strategia aziendale per supportare i vostri clienti in ottica GDPR.



Una volta che voi e i vostri clienti avrete colto l'impatto e le implicazioni del GDPR sulle vostre aziende, ci saranno probabilmente svariate opportunità per aggiornare e integrare nuove tecnologie e soluzioni e rinnovare quindi i servizi di sicurezza dei vostri Clienti. Ed è qui che Metha Group può aiutarvi e supportarvi con la soluzione vendor più adatta a voi.

I 5 pilastri Metha Group per il vostro successo

ECCELLENZA ESECUTIVA

Una cultura della performance che dà la certezza che faremo sempre il meglio possibile.

SOLUZIONI E SERVIZI

Un portafoglio di prodotti, servizi e soluzioni cloud all'avanguardia in grado di soddisfare ogni vostra esigenza.

SUCCESSO DEL CLIENTE

Noi consentiamo alla vostra azienda di aumentare la redditività del proprio business.

SQUADRA VINCENTE

Le persone altamente motivate e responsabilizzate sono alla base della nostra cultura vincente.

DIGITAL ENABLEMENT

Sarà più facile collaborare con noi, sia per voi che per i vostri Vendor. I nostri strumenti e la nostra data analytics saranno un fattore chiave di distinzione

Contattaci all'indirizzo
marketing@methagroup.it
oppure
chiamaci al numero
(+39) 02- 87087107

METHA GROUP®
IT Around Your Business