YOUR BUSINESS PROTECTION

PREVENZIONE LEGALE
INVESTIGAZIONE
COMPLIANCE

SICUREZZA DELLE INFORMAZIONI

PREPARAZIONE AL GDPR

Il General Data Protection Regulation (GDPR) è la risposta dell'Unione Europea al ruolo enormemente esteso che la tecnologia riveste attualmente nella vita di tutti i giorni. Il GDPR è stato ratificato dagli stati membri nell'aprile del 2016 ed è entrato in vigore lo scorso 25 maggio 2018.
Pur essendo un Regolamento UE, si applica a qualsiasi organizzazione che raccolga dati personali di residenti dell'UE, indipendentemente dalla sua ubicazione fisica.
Obiettivo del nuovo Regolamento è garantire che nel processo di raccolta di dati personali sia integrata un'adeguata protezione dei dati "per impostazione predefinita fin dalla progettazione". Ciò ha inizio con una raccolta limitata ai dati minimi necessari per una finalità specifica e con la cancellazione dei dati quando non sono più necessari. Un altro importante aspetto del GDPR è che l'interessato, la fonte dei dati personali, è il proprietario di tali dati. In qualità di proprietario, l'interessato deve avere la possibilità di revocare il proprio consenso alla raccolta dei dati con la stessa facilità con la quale ha concesso l'autorizzazione.
L'interessato ha inoltre il "diritto all'oblio" e ad acquisire i propri dati personali.
Il GDPR definisce poi le condizioni che richiedono l'invio di una notifica in caso di violazione dei dati e prevede due livelli di sanzioni a seconda della gravità della violazione.

In considerazione dei rapidi cambiamenti tecnologici, il GDPR impone l'onere di una "valutazione continuativa dei rischi" all'organizzazione che raccoglie i dati (il titolare del trattamento) e richiede la conformità al regolamento di qualsiasi organizzazione esterna che tratti i dati (responsabile del trattamento).

CHE COS'E' IL GDPR?

La continua digitalizzazione e globalizzazione della nostra economia fa sempre più affidamento sul controllo e l'elaborazione dei dati personali. Da una parte ciò offre enormi opportunità di business, dall'altra si accompagna a una crescente sensibilizzazione e preoccupazione pubblica relativamente all'importanza della protezione dei dati personali.

Un recente sondaggio condotto da KPMG International su scala mondiale ha rivelato che più della metà (il 55%) dei consumatori ha affermato di aver abbandonato gli acquisti online a causa di preoccupazioni sulla privacy. Il sondaggio indica anche che meno del 10% degli intervistati ritiene attualmente di avere il controllo sul modo in cui le organizzazioni gestiscono e utilizzano i loro dati personali.

Il General Data Protection Regulation (GDPR) dell'Unione Europea nasce in risposta a queste preoccupazioni. Riconoscendo il valore di tali dati, il regolamento impone un costo sulla loro raccolta, conservazione e utilizzo, attribuendo alle organizzazioni la responsabilità della loro protezione e obbligandole a restituirne il controllo e la proprietà alle persone.

A differenza della direttiva esistente sulla protezione dei dati, la 95/46/CE, che è stata recepita nelle singole legislazioni nazionali, GDPR è una disposizione unitaria mirante a rafforzare, unificare e applicare la protezione dei dati personali nell'intera UE. I suoi criteri più rigorosi, obblighi aggiuntivi e sanzioni per mancata conformità più elevate (il valore più grande tra il 4% del fatturato mondiale e 20 milioni di euro) faranno indubbiamente aumentare sia l'impegno richiesto per il raggiungimento della conformità, sia i rischi associati alla mancata conformità.

L'aspetto positivo è che si tratta, in gran parte, di un'azione unificata tesa a definire le responsabilità delle organizzazioni in merito alla protezione dei dati in tutti gli Stati membri dell'Unione.

CHI È INTERESSATO?

Il GDPR si applica a qualsiasi organizzazione, in qualsiasi paese, che raccoglie, conserva o tratta i dati personali di residenti dell'Unione europea. Questi dati possono provenire da dipendenti, business partner, clienti attuali e potenziali.

Nella terminologia del regolamento, tali organizzazioni sono dette "titolari del trattamento", che determinano come e perché sono trattati i dati personali, o "responsabili del trattamento", che agiscono per conto dei titolari. Per entrambi il GDPR stabilisce maggiori obblighi e prevede sanzioni in caso di violazione.

QUALI SONO LE IMPLICAZIONI PER LE IMPRESE GLOBALI?

Per la maggior parte delle imprese, le implicazioni sono rilevanti e di ampia portata, con la necessità di cambiamenti che coinvolgono i flussi di elaborazione dei dati, la struttura organizzativa, i processi aziendali, fino alle tecnologie informatiche e di sicurezza.

DIRITTI DELLE PERSONE

L'essenza del GDPR è la definizione dei diritti delle persone in relazione alla protezione dei dati. Tali diritti possono essere sintetizzati come segue:

- **Consenso informato**

Il diritto di essere chiaramente informato sui motivi che richiedono la comunicazione dei dati e sulle modalità del loro utilizzo. Il consenso deve essere accordato in modo esplicito e può essere ritirato in qualsiasi momento.

- **Accesso**

Il diritto di accedere gratuitamente a tutti i dati raccolti e di ottenere conferma delle modalità del loro trattamento.

- **Correzione**

Il diritto di correggere i dati se inaccurati.

- **Cancellazione e "diritto all'oblio"**

Il diritto di richiedere la cancellazione dei propri dati.

- **Portabilità dei dati**

Il diritto di recuperare e riutilizzare i dati personali, a dati personali in base a questi diritti.

Parte impegnativa di tale sfida sarà già solo il raggiungimento di un punto in cui l'organizzazione sia in grado di individuare con precisione tutte le istanze dei dati di una persona nell'intera infrastruttura (ossia il problema del "**Dove sono i miei dati?").**

Per alcune organizzazioni, ciò offrirà l'opportunità di ottimizzare le operazioni, eliminare raccolte di dati non necessari e limitare il trattamento ai soli dati essenziali per gli obiettivi fondamentali dell'impresa. In ogni caso, la transizione alla conformità sarà probabilmente un impegno significativo.

RESPONSABILIZZAZIONE E GOVERNANCE

L'organizzazione deve quindi essere in grado di dimostrare la conformità tramite opportune misure di governance, che includano documentazione dettagliata, registrazione e valutazione continua del rischio.
A questo proposito vi è un'aspettativa aggiuntiva di "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita": la sicurezza deve cioè, nella misura maggiore possibile, essere parte integrante di tutti i sistemi sin dall'inizio, piuttosto che qualcosa applicata a posteriori, anche se questo chiaramente presenta una sfida enorme dove sono coinvolti sistemi legacy. Casi del genere rendono evidente il ruolo essenziale, come primo livello di difesa, della sicurezza a livello di rete, che può rappresentare l'unica difesa dalla violazione dei dati per l'enorme numero di sistemi legacy ancora in uso, finché questi non potranno essere riprogettati con misure intrinseche di protezione dei dati.
Oltre alle precauzioni più ovvie quali la cifratura dei dati, la pseudonimizzazione e così via, il GDPR usa termini quali "adeguato" e "stato dell'arte" per descrivere il requisito di una continua valutazione del rischio e dell'aggiornamento delle misure di conformità.
Con la scoperta di nuove vulnerabilità, per rimanere conformi in futuro può essere necessario cambiare la tecnologia della sicurezza o le pratiche di protezione dei dati considerate oggi conformi.

Se da una parte ciò lascia indubbiamente spazio a dispute legali sull'interpretazione della norma, dall'altra le organizzazioni dovranno Propri scopi, tra diversi servizi.
La prima sfida da affrontare per la conformità al GDPR è quindi quella di controllare e, se necessario, modificare il modo in cui l'organizzazione raccoglie, conserva e tratta i

NOTIFICA DELLE VIOLAZIONI

Il GDPR introduce inoltre per le organizzazioni un nuovo obbligo di notifica alle autorità competenti di qualsiasi violazione dei dati personali che possa avere come conseguenza un rischio per "i diritti e le libertà delle persone fisiche". Quando il rischio è considerato "elevato", la notifica deve essere estesa anche agli interessati. La notifica deve essere effettuata "senza ingiustificato ritardo" e, ove possibile, entro 72 ore dalla scoperta dell'evento.
Anche in assenza di riferimenti espliciti a specifiche tecnologie di protezione dei dati e sicurezza di rete, la transizione alla conformità deve iniziare con la verifica che la rete sottostante sia sufficientemente protetta da tutti i possibili vettori di attacco.

SFIDE RELATIVE ALLA SICUREZZA DELLE RETI

MANTENERE DIFESE "ALLO STATO DELL'ARTE"

Tenere il passo con l'evoluzione del panorama delle minacce costituisce una sfida anche senza la condizione posta dal GDPR in merito a difese "allo stato dell'arte". Gli enormi proventi della criminalità informatica, per non parlare del potenziale terrorismo sponsorizzato da stati, assicura un livello di risorse e innovazione che può essere difficile da eguagliare per qualsiasi singola impresa o persino per governi nazionali.

Comunque adottare meccanismi per garantire che le loro iniziative siano **allineate alle più recenti innovazioni tecnologiche** e alla conseguente evoluzione delle minacce.

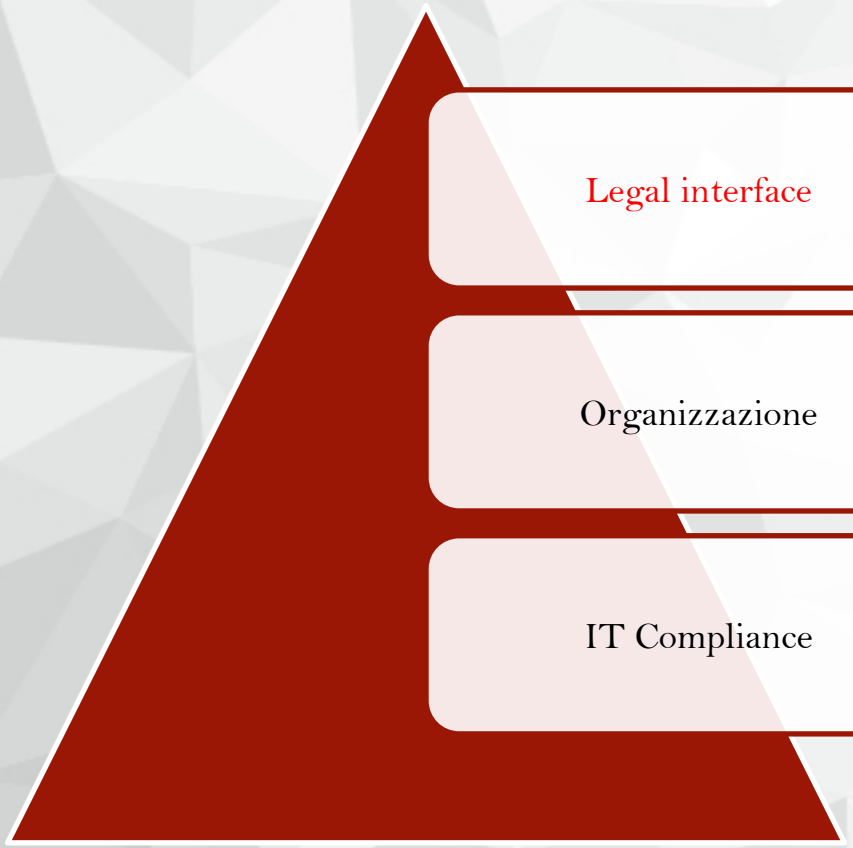
NOTIFICARE LE VIOLAZIONI ENTRO 72 ORE

La prima sfida comportata dal requisito del GDPR di notifica delle violazioni consiste nel rilevare quando si verifica una violazione che rientra nella definizione e determinare quali risorse possono essere a rischio. Quasi per definizione, qualsiasi violazione esterna della sicurezza che raggiunga il suo scopo deve avere evaso completamente i meccanismi di rilevamento, oppure non essere stata rilevata con sufficiente tempestività. Ciò significa che ha sfruttato un meccanismo di attacco diverso da tutti quelli rilevati in precedenza, oppure che i segnali di allarme che ha generato non sono stati colti.

È un fatto che, nel 2016, il tempo medio impiegato dalle organizzazioni per scoprire una violazione tipica sia stato di quasi cinque mesi. Fortunatamente, la finestra di 72 ore prevista dal GDPR si apre al momento del rilevamento, non al momento dell'intrusione. Tuttavia, poiché l'impatto finanziario di una violazione è fortemente correlato al tempo di cui l'hacker dispone per accedere ai sistemi, l'abbreviazione del tempo di rilevamento resta una necessità fondamentale.

Ovviamente, è impossibile rilevare ciò che non è rilevabile; gli amministratori della sicurezza devono pertanto accettare il fatto che occasionalmente può verificarsi un'intrusione e prepararsi di conseguenza, puntando al tempo stesso alla massima riduzione di tali eventi e all'accelerazione del loro rilevamento con ogni mezzo possibile. Come accennato in precedenza, il GDPR non richiede la notifica di tutte le violazioni della sicurezza, ma solo di quelle che presentano un rischio per i diritti delle persone.

Pertanto, se i dati violati sono stati adeguatamente offuscati tramite crittografia o pseudonimizzazione e se la durata dell'accesso non autorizzato è mantenuta breve, il rischio per tali diritti dovrebbe essere minimo.



Legal interface

- INFORMATIVA
- LETTERE DI NOMINA
- VERIFICA INFORMATIVA SITO

Organizzazione

- SVILUPPO REGISTRO TRATTAMENTO
- ANALISI IMPATTI (PIA)

IT Compliance

- ASSETS INVENTORY
- PROFILAZIONE
- BACK-UP
- ANTI MALWARE
- CRIPTOGRAFIA
- FIREWALL
- PROCEDURA DATA BREACH
- **CERTIFICAZIONE COMPLIANCE**

AUTORIZZAZIONE PREFETTURA DI NOVARA
N. 0043949 PROT. N. 7028/1.28.7/O.S.P. del 18.-07-2016

Dott.ssa Marilena Guglielmetti

CONSULENTE DI COMPLIANCE AZIENDALE

INVESTIGATORE CRIMINOLOGO

M – Investigation S.r.l.

28100 Novara • Via Giovannetti n°8 ang. via Dei Gautieri

+39 0321 32250 - +39 338 44 36 770

mguglielmetti@minvestigation.it • www.minvestigation.it