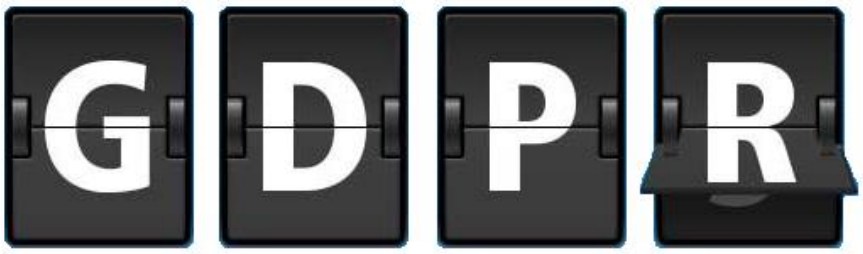
Pillole sul .....



25 maggio 2018

Sommario

Enterprise Solutions S.r.l. : Largo Luigi Cossa, 9 - 00148 Roma
Uff. +39 06 99340131 - **Fax** +39 06 98380224

P.IVA e C.F. 09384011004 - Cap. Sociale Euro 30.000,00 i.v. - CCIAA n. 1159182

Protezione delle risorse web basata su prove: un elemento imprescindibile del regolamento GDPR

I GDPR: che cos'è?

Il Regolamento generale per la protezione dei dati (GDPR) dell'Unione Europea è un nuovo regolamento UE che sostituisce l'attuale direttiva sulla protezione dei dati 95/46/CE, nonché numerose leggi locali di attuazione della direttiva stessa. Il GDPR armonizza le leggi sulla privacy dei dati di tutta Europa, al fine di proteggere i diritti di tutti i cittadini UE alla privacy dei dati.

In base alle nuove regole fissate dal GDPR, l'impatto della mancata conformità (ad esempio, la mancata dimostrazione che i dati personali oggetto del trattamento sono stati adeguatamente protetti in caso di violazione) può avere un impatto rilevante sulla situazione finanziaria di un'organizzazione, nonché gravi conseguenze per i suoi dirigenti. In definitiva, è messa in gioco la reputazione dell'organizzazione stessa.

Il GDPR sarà applicato da tutti gli stati membri dell'UE ed entrerà in vigore a partire dal 25 maggio 2018. Tra i suoi numerosi requisiti, il GDPR richiede che le imprese, al fine di ridurre al minimo i rischi per i diritti e le libertà fondamentali delle persone fisiche, introducano "misure tecniche ed organizzative appropriate al fine di garantire un livello di sicurezza adeguato al rischio". Queste misure di sicurezza devono essere implementate prima della scadenza di maggio 2018. Dato il notevole volume di dati personali e dati sensibili accessibili attraverso siti web e applicazioni che interagiscono con Internet, non si tratta certo di un compito semplice.

Il GDPR, inoltre, impone alle organizzazioni che trattano dati personali di essere in grado dimostrare che sono poste in essere "adeguate" misure di sicurezza volte a proteggere in modo efficiente ed efficace i dati personali elaborati.

L'adempimento di quest'obbligo è complicato dal fatto che le organizzazioni fanno spesso ricorso a terzi per fornire specifiche attività di elaborazione dati. Mentre ci può essere una catena di attività di elaborazione dei dati distribuita tra un determinato numero di parti distinte, l'organizzazione originaria, il cosiddetto "Responsabile del controllo dei dati", rimane, appunto, responsabile della protezione dei dati personali trattati. Data la responsabilità stabilita in forza del GDPR, è assolutamente necessario che i Responsabili del controllo dei dati dispongano di adeguate misure di sicurezza e siano in grado di fornire la prova che queste misure sono efficaci, specialmente nel malaugurato caso di una perdita di dati o di una violazione.

Che cos'è esattamente una "misura di sicurezza adeguata" e quali prove necessarie ci si aspetta che siano fornite in modo tempestivo? In conformità al GDPR, per adeguate misure di sicurezza si intendono quelle misure che tengono conto dello stato dell'arte, del costo di realizzazione e di fattori quali il campo di applicazione, il contesto e le finalità del trattamento, controbilanciandoli con i rischi e l'impatto sui diritti e sulla libertà delle persone. Naturalmente la percezione di ciò che è "appropriato" o "equilibrato" sarà determinata dal Garante per la protezione dei dati personali (Data Protection Authority DPA), che certamente considererà le best practice del settore come punti di riferimento.

Enterprise Solutions S.r.l. : Largo Luigi Cossa, 9 - 00148 Roma
Uff. +39 06 99340131 - **Fax** +39 06 98380224

P.IVA e C.F. 09384011004 - Cap. Sociale Euro 30.000,00 i.v. - CCIAA n. 1159182

Uno strumento per arrivare al necessario equilibrio discusso in precedenza è la valutazione dell'impatto sulla protezione dei dati (Data Protection Impact Assessment o DPIA), una procedura necessaria in alcuni casi in forza del GDPR per determinare il potenziale impatto delle attività di elaborazione dei dati. Quando si conduce una DPIA, un'organizzazione deve documentare nel dettaglio una serie di fattori, tra cui:

- Previste operazioni di elaborazione dei dati;
- La necessità e la proporzionalità di tali operazioni;
- Una valutazione dei rischi di violazione dei dati associati alle operazioni;
- Le misure previste per affrontare questi rischi, comprese le misure di sicurezza e di protezione, e meccanismi per garantire la protezione dei dati personali.

Il GDPR impone un approccio alla protezione dei dati basato sul rischio. Gli obblighi di sicurezza non sono fissati in modo avulso dalla realtà, ma devono piuttosto essere sviluppati basandosi su un'approfondita analisi e comprensione dei rischi che ogni attività di elaborazione può avere per le persone i cui dati vengono trattati. Mentre questo approccio offre la flessibilità necessaria per consentire alle organizzazioni di applicare misure ragionevoli alla luce di costi, architettura di sistema e fattori correlati, esso richiede, tuttavia, una rigorosa analisi costi-benefici/rischi riferita a tutto ciò che l'organizzazione fa con i dati personali. In molti casi, si tratta di un compito importante e impegnativo.

La misura in cui un'organizzazione è in grado di fornire con successo prove sufficienti in merito all'adozione di un sistema efficace di riduzione dei rischi dipenderà dalla sua comprensione dei rischi relativi alla privacy, nonché dei punti di forza delle misure di sicurezza "all'avanguardia" che sceglie di implementare in risposta ai rischi percepiti.

Naturalmente, il successo di un'organizzazione dipenderà anche dalla selezione di partner che comprendano a fondo gli obblighi inerenti alla sicurezza e alla protezione dei dati e siano in grado di adottare le misure necessarie per proteggere i propri sistemi.

In che modo EnterpriseSolutions può agevolare la conformità al GDPR?

In base al GDPR, è necessario raccogliere prove per dimostrare che i dati personali trattati da un'organizzazione siano adeguatamente e sufficientemente protetti. In un mondo interconnesso in cui molte applicazioni e siti web contengono dati personali o permettono di accedere ad essi, questa può essere una grande sfida. Questa sfida coinvolge il personale, i processi e la tecnologia.

Enterprise fornisce quattro principi per acquisire familiarità con i requisiti di sicurezza previsti dal GDPR. Di seguito, verrà descritto come Enterprise Solutions possa aiutare le organizzazioni ad affrontare i grandi rischi legati all'elaborazione dei dati.

Lavorare basandosi sui rischi

Notevoli volumi di dati personali vengono elaborati attraverso applicazioni connesse a Internet.
In forza del GDPR, alle aziende e alle organizzazioni è richiesto di implementare adeguate misure tecniche ed organizzative per proteggere i dati personali che si trovano sotto il loro controllo.
Tali misure dovrebbero includere tecnologie di sicurezza progettate per proteggere applicazioni connesse a Internet e siti web da attacchi volti ad accedere a dati personali.

Enterprise Solutions S.r.l. : Largo Luigi Cossa, 9 - 00148 Roma
Uff. +39 06 99340131 - **Fax** +39 06 98380224

P.IVA e C.F. 09384011004 - Cap. Sociale Euro 30.000,00 i.v. - CCIAA n. 1159182

Enterprise suggerisce un servizio di protezione dalle minacce basato sul rischio. Esso è costruito da "gruppi di rischio" che possono essere utilizzati per mitigare in modo immediato ed efficace i rischi associati ai più sofisticati attacchi. Implementando un servizio di protezione adeguato offre ai clienti la possibilità di dimostrare di aver preso misure ragionevoli contro minacce conosciute e 0 day.

Costruire le prove

In caso di una violazione della protezione che richieda la segnalazione della perdita di dati personali a un DPA, è estremamente importante che sia fornita al DPA la prova delle misure di mitigazione già adottate e di quelle che si adotteranno in futuro per garantire che l'impatto sia minimo.

Affinché le misure di sicurezza necessarie siano efficaci, devono essere costantemente riesaminate a fronte di nuove e mutevoli minacce. Enterprise Solutions aiuta le organizzazioni a rispondere al panorama delle minacce in continua evoluzione e fornisce la prova che esse hanno attivamente anticipato e mitigato i rischi, creando e mantenendo regole efficienti ed efficaci.
Un esperto di sicurezza analizzerà le politiche di sicurezza e formulerà suggerimenti per mantenere costantemente adeguate le regole aziendali.

Usare una tecnologia "all'avanguardia"

In conformità al GDPR, per adeguate misure di sicurezza si intendono quelle misure che tengono conto del livello tecnologico, del costo di realizzazione e di fattori quali il campo di applicazione, il contesto e le finalità del trattamento, controbilanciandoli con i rischi e l'impatto sui diritti e sulla libertà delle persone.

Naturalmente, la percezione di ciò che è "appropriato" o "equilibrato" sarà determinata dal Garante per la protezione dei dati personali (Data Protection Authority o DPA) che, certamente, considererà le best practice del settore come punti di riferimento.

I furto delle credenziali (username/password) può molto facilmente condurre alla perdita di dati personali sensibili. A seguito di una recente grande perdita di password su Internet, i ricercatori hanno rilevato che l'8,8% di queste credenziali fa uso di sette password molto semplici (ad esempio, 123456, password, ecc.). Le persone tendono a scegliere password semplici che possono facilmente ricordare e riutilizzano spesso le stesse password. Una volta che le credenziali sono "attaccate", è possibile che più fonti di dati siano esposte. I pirati informatici utilizzano sofisticati botnet per accedere in modo rapido e automatico a siti web di tutto il mondo utilizzando credenziali rubate.

Implementare una strategia per la sicurezza aziendale consente di semplificare il processo di conformità GDPR ed evitare i costi associati.

Non bisogna fidarsi di niente e di nessuno né all'interno né all'esterno di un ambiente aziendale.
Gli accessi devono essere esplicitamente concessi e confermati a tutte le risorse da un sistema di gestione centralizzato e tutto il traffico deve essere monitorato e controllato permanentemente al fine di evitare anche solo per errori umani la perdita del dato.

Usare una formazione adeguata al personale

Tenere sempre aggiornato il personale delle possibili minacce che si possono incontrare semplicemente facendo il nostro lavoro è una delle fonti più importanti misure di sicurezza per l'eliminazione degli incidenti.

Enterprise Solutions S.r.l. : Largo Luigi Cossa, 9 - 00148 Roma
Uff. +39 06 99340131 - **Fax** +39 06 98380224

P.IVA e C.F. 09384011004 - Cap. Sociale Euro 30.000,00 i.v. - CCIAA n. 1159182

Conclusione

Il GDPR richiede un approccio alla protezione dei dati basato sul rischio e chiede la prova evidente che i rischi sono costantemente mitigati in misura sufficiente.

Tutte le organizzazioni che elaborano in qualche modo i dati personali di soggetti nell'UE devono essere preparate a dimostrare di aver adottato misure forti volte a proteggere i dati personali sotto il loro controllo. Sfruttare le conoscenze e l'esperienza di professionisti in materia di sicurezza aiuta i clienti a proteggere le proprie risorse, compresi i dati personali protetti secondo il GDPR contro la perdita e l'accesso illegale.

Enterprise Solutions può aiutare con misure concrete ad aumentare gli sforzi dei clienti volti a raggiungere la piena conformità al GDPR.

Con i suggerimenti più appropriati, i clienti possono dimostrare di aver intrapreso passi concreti per prepararsi ad affrontare molte minacce conosciute e 0 day.

Alcuni punti cruciali richiesti dalla normativa

Articolo GDPR	Ambito di applicazione
28 e 30	Gestione Unificata delle identità, delle utenze applicative dell'accesso e visibilità dei dati strutturati (DB) e non strutturati (Fileshare e cloud)
32,33 e 34	Securizzazione dei dati e delle credenziali di accesso ai sistemi
24 e 25	Protezione da attacchi esterni tramite firewall perimetrali, APT anti-ransomware ecc…
24 e 25	Protezione del data Exfiltration (DNS, Behavioral Analysis, DLP)
33 e 35	Gestione degli eventi (Monitoring, SIEM, Log Management)
32 e 33	Servizi di Change Management, Incident Management
25,33,34,35 3 36	Progettazione e Privacy by design, reporting

Documentazione richiesta dal GDPR

- Modelli standard per informativa e raccolta del consenso
- Designazione del/-i Responsabile/-i* e degli incaricati del trattamento
- Designazione ed elenco degli Amministratori di sistema
- Designazione del DPO**
- Risk Analysis
- Privacy Impact Analysis**
- Piano di rientro
- Registro dei trattamenti***
- Disciplinare interno
- Archivio delle violazioni
- Attestato di Formazione

Enterprise Solutions S.r.l. : Largo Luigi Cossa, 9 - 00148 Roma
Uff. +39 06 99340131 - **Fax** +39 06 98380224

P.IVA e C.F. 09384011004 - Cap. Sociale Euro 30.000,00 i.v. - CCIAA n. 1159182

Sanzioni 1/1:

fino a € 10.000.000,00, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore nei casi di violazione degli artt. 8, 11, 25, 28, 30, 32, 33, 35, 36, da 37 a 39, in particolare:

- violazione degli obblighi in materia di privacy by design e privacy by default
- violazione dell'obbligo di tenuta del registro dei trattamenti
- violazione delle disposizioni in materia di sicurezza
- violazione dell'obbligo di notifica nei casi di violazione dei dati personali
- violazione delle disposizioni in materia di PIA e di consultazione preventiva
- violazione delle prescrizioni in tema di DPO

Sanzioni 1/2:

fino a € 20.000.000,00, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore nei casi di violazione degli artt. 5, 6, 7, 9, da 12 a 22, da 44 a 49, tutto il Capo IX, art. 58 §1, in particolare:

- violazione dei principi applicabili al trattamento dei dati (compliance)
- violazione dell'obbligo di informativa e dei diritti degli interessati
- violazione obblighi connessi al trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali
- inottemperanza agli ordini dell'Autorità di controllo*

Una buona analisi

L'Analisi del rischio ha l'obiettivo di individuare e valutare il danno provocato agli asset di un'organizzazione e di individuare possibili contromisure per mitigare i rischi evidenziati.

- ***Obiettivi:***
  1. Quantificare l'impatto in relazione ai possibili scenari di rischio;
  2. Identificare vulnerabilità e minacce;
  3. Individuare l'impatto del rischio e le possibili contromisure necessarie a mitigarlo.

Il nostro obiettivo è aiutare i titolari di aziende a gestire i rischi cui si va incontro con il nuovo regolamento sulla privacy.

Grazie per l'attenzione!

Enterprise Solutions S.r.l. : Largo Luigi Cossa, 9 - 00148 Roma
Uff. +39 06 99340131 - **Fax** +39 06 98380224

P.IVA e C.F. 09384011004 - Cap. Sociale Euro 30.000,00 i.v. - CCIAA n. 1159182