S.I.P.E.
SOLUZIONI INFORMATICHE PERSONALIZZATE
www.sipe.it

IBM Gold Business Partner

GDPR

Il Regolamento Generale sulla Protezione dei Dati

INDICE

Lo scenario
Privacy: what's happening?

I cambiamenti imposti dall'innovazione tecnologica hanno generato un livello senza precedenti di raccolta e di elaborazione di dati, destinato a subire un'ulteriore espansione con le nuove applicazioni dell'Internet delle cose, della robotica, della realtà aumentata.

Dalle parole e dai numeri ai giochi, ai media, alle funzioni complesse dei sistemi industriali, all'ambiente, ai trasporti: tutto quello che riguarda la nostra esistenza ha subito una trasformazione digitale.

Lo sviluppo delle tecnologie rappresenta il presupposto essenziale perché le imprese possano competere nella dimensione globale dei mercati e perché possano migliorare le condizioni di vita delle persone in ogni angolo del pianeta.

Ma i progressi incessanti di questi cambiamenti mettono in discussione molti paradigmi e sollevano interrogativi ineludibili.

Lo sviluppo di una florida economia fondata sui dati sfrutta le funzionalità tecnologiche per la loro raccolta continua e massiva, la trasmissione istantanea ed il riutilizzo.

Ciò ci espone a nuovi rischi.

Poiché i dati rappresentano la proiezione digitale di persone e imprese, aumenta in modo esponenziale anche la nostra vulnerabilità.

Da un lato le imprese tecnologiche hanno dilatato la raccolta e la disponibilità dei nostri dati, dall'altro le esigenze di sicurezza, di fronte alla minaccia criminale e terroristica, hanno spinto progressivamente i governi ad estendere il controllo delle attività svolte in rete per finalità investigative in modo sempre più massivo.

In occasione dell'ultimo Privacy Day Antonello Soro, presidente del Garante della Privacy, ha detto:

«La capacità di estrarre dai dati informazioni che abbiano un significato e siano funzionali, richiede infatti lo sviluppo di sofisticate tecnologie e di competenze interdisciplinari che operino a stretto contatto».

E ha aggiunto: «Le riforme del quadro giuridico europeo rappresentano una svolta importante per definire un contesto uniforme e proiettato sulle esigenze future e, soprattutto, preservare la fiducia degli utenti nello spazio digitale e nelle sue potenzialità. Fiducia, innovazione e futuro sono fortemente correlati".

GDPR: La norma
Che cos'è?

Il Regolamento Generale sulla Protezione dei Dati (GDPR) è la nuova normativa europea che armonizza e supera le normative attualmente vigenti negli Stati facenti parte della Comunità Europea, punta a rafforzare e proteggere da minacce presenti e future i diritti alla protezione dei dati sensibili dei propri cittadini, dentro e fuori dall'Unione Europea.

Per farlo, il GDPR introduce nuovi obblighi e nuove sanzioni che impongono alle aziende l'adozione di specifiche misure per la protezione dei dati personali.

Questo impone alle aziende l'urgenza di indirizzare correttamente i propri investimenti verso adeguati strumenti informatici e procedurali al fine di ridurre il rischio di pesanti sanzioni pecuniarie e integrarli alle nuove polizze assicurative per la copertura degli eventuali danni propri e a terzi.

Tra gli elementi introdotti dalla normativa ci sono la necessità di gestire un registro dei trattamenti e garantire nel tempo la sicurezza dei dati, l'obbligo di notificare i data breach, l'esigenza di introdurre la figura del Data Protection Officer, l'esigenza di adottare un approccio ispirato al principio di "privacy by design" e le già citate nuove aspre sanzioni.

C'è tempo fino al 25 maggio 2018, ma la portata innovativa del regolamento è imponente.

Chi ha tempo non lo butti via, bensì lo utilizzi per governare al meglio il processo che conduce alla compliance e colga l'opportunità di adottare procedure e tecnologie che oltre a garantire il rispetto della normativa accrescano il livello di sicurezza e la continuità operativa.

La principale differenza, rispetto al passato, è che gestire la "privacy" all'interno dell'organizzazione non potrà più essere un semplice adempimento, a volte più formale che sostanziale, ai singoli obblighi normativi.

Implicherà di impostare un processo, analizzare i rischi e gestire, nel tempo, con continuità e nel fermo rispetto dei diritti di ogni individuo, i dati personali che si trattano.

La normativa prevede una multa fino a 20 milioni di euro o il 4% del fatturato annuo globale per ogni caso di violazione nei seguenti casi:

- Per chi non si adegua alla nuova normativa entro il termine previsto dalla Comunità Europea;

- Nei casi in cui, nonostante l'adempimento, emergono carenze regolamentari a seguito di una violazione dei dati.

La compliance in 5 punti
Le fasi del cambiamento

Le attività fondamentali per preparare la tua azienda a fronteggiare il cambiamento:

- Comprendere come i nuovi obblighi previsti da GDPR impatteranno sulle attività
- Determinare quali sono e dove si trovano i dati sensibili e come sono messi in sicurezza
- Nominare un Data Protection Officer, dove necessario
- Rivedere tutte le informative sulla privacy
- Rivedere i processi di accesso ai dati, rettifica e cancellazione richieste dalle persone interessate

Ecco cinque punti da cui partire.

1 CONSAPEVOLEZZA

È opportuno conoscere tutte le vulnerabilità dell'azienda, avviando un'indagine approfondita di tutti i sistemi interni e/o esterni per avere piena consapevolezza delle fragilità e dei rischi a cui si è esposti, in modo da proteggere i dati e agevolare il processo di conformità.

2 MAPPATURA DEI DATI

Necessaria per analizzare la portabilità dei dati, i diritti di accesso e di cancellazione. Per creare una buona mappatura è necessario scoprire e classificare i dati personali, le prime informazioni da proteggere. La conoscenza dei dati è alla base di GDPR, "You cannot protect what you don't know about."

Cosa si intende per "Personal Data"?

I dati personali sono tutte le informazioni che si riferiscono ad una persona identificata o identificabile.

Cosa si intendere per identificabile?

È la persona fisica che può essere individuata direttamente o indirettamente. In quest'ultimo caso, non si considera quindi "Dato Personale" solamente un'informazione univoca di un individuo (per es. il nome, l'email, il codice fiscale, etc.) ma anche un insieme di dati generici, che se correlati tra loro possono ricondurre a uno specifico individuo.

3 MONITORAGGIO

È fondamentale considerare il diritto delle persone di tracciare i dati di accesso, modificarli, cancellarli o trasferirli.

Gli individui possono richiedere alle organizzazioni che possiedono dati sul loro conto, il diritto di rettificare, cancellare o trasferire i dati. "Il regolatore dovrebbe essere obbligato a rispondere alle richieste della persona, senza indebito ritardo e al più tardi entro un mese.

Perché è importante: Le multe più alte di GDPR sono per la violazione dei diritti della persona interessata, come per la mancata risposta o la fornitura di informazioni adeguate.

L'interessato ha inoltre il diritto al risarcimento monetario dei danni.

Le aziende hanno quindi bisogno di strumenti per dimostrare che le richieste vengono processate in modo tempestivo.

4 SICUREZZA

La messa in sicurezza dei dati personali non potrà più essere presa alla leggera: rispetto alla normativa italiana prevista dal Garante della Privacy, il testo europeo innalza significativamente il livello di protezione dei dati richiesto.

Per la norma approvata dalla Comunità Europea "occorre attuare misure tecniche e organizzative per garantire un livello di sicurezza adeguato".

Cosa si intende?
Il testo pone l'attenzione su "i rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati."

Tra le misure di protezione contemplate dalla legge, si annovera:

- La pseudonimizzazione e la cifratura dei dati personali;
- La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento.

Si introduce inoltre il principio di "Data Protection By Design" che obbligherà da un lato a verificare e garantire il corretto livello di protezione, dall'altro l'assenza di vulnerabilità per i sistemi e per le applicazioni che tratteranno i dati sensibili già in fase di progettazione.

5 NOTIFICA

Sarà importante segnalare le violazioni in modo tempestivo. Nel caso di una violazione dei dati personali il responsabile del trattamento, senza indebito ritardo (entro e non oltre 72 ore dopo l'avvenimento), deve comunicare tale violazione all'autorità di vigilanza.

Come previsto dall'articolo 33, la comunicazione al Garante deve contenere:
- La descrizione della violazione
- La natura dei dati interessati
- Le probabili conseguenze della violazione

- Le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e/o per attenuare i possibili effetti negativi.

In sostanza "il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio."

Questa documentazione consentirà all'autorità garante di verificare il rispetto della norma da parte del titolare del trattamento dei dati.

Tutto ciò che devi sapere su **Infographics**

Il **regolamento generale sulla protezione dei dati (GDPR)** è stato pubblicato il 4 maggio 2016, e sarà immediatamente applicabile dopo un periodo di transizione di due anni, il **25 maggio 2018**, per qualsiasi organizzazione che opera nel mercato europeo.

DATA PROTECTION

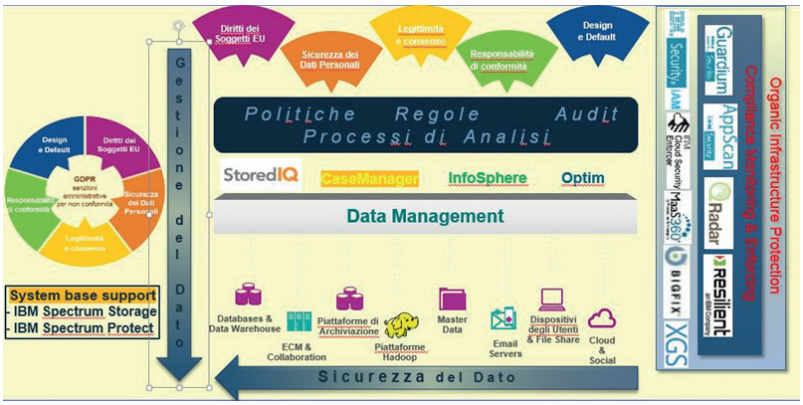
A differenza della Direttiva esistente del 1995 sulla protezione dei dati, il GDPR cercherà di creare un quadro di legge armonizzato e unificato per tutti i paesi dell'UE.

LO SAI?

*Gli obiettivi del GDPR sono quelli di restituire ai cittadini il **controllo dei propri dati** personali e semplificare il contesto normativo che riguarda gli affari internazionali.*

Il mercato rispetto delle norme prevede pesanti multe (anche fino a 20 milioni di euro). Questo è il momento di costruire sulle fondamenta di cui disponi per garantirti **protezione**, **controllo** e **conoscenza** dei tuoi dati.

IBM:
l'offerta più completa a supporto della compliance



La normativa GDPR introduce nuovi diritti e doveri per i cittadini europei e le aziende che raccolgono i loro dati.

Per le Aziende, come specificato sopra, è particolarmente onerosa la eventuale multa per inadempienza, fino a 20 milioni di euro o il 4% del totale fatturato annuo in tutto il mondo.

IBM propone l'adozione di soluzioni di Business Analytics che possono occuparsi Gestione del Dato per poter aiutare le Aziende ad operare nel rispetto della legge ottemperando ai 5 concetti principali:

- Diritti dei soggetti UE: la cancellazione, l'accesso e la portabilità dei dati
- Sicurezza dei dati personali: garantire un livello di sicurezza adeguato al rischio, facilitando reazioni veloci a incidenti e l'identificazione dei dati a cui si accede per ridurre il rischio
- Legittimità e consenso: monitoraggio dei processi per dare / revocare il consenso al trattamento dei dati, l'implementazione di una singola fonte di verità per i dati personali ed il collegamento con i sistemi che li trattano
- Responsabilità di conformità: la necessità di dimostrare la conformità con i principi relativi al trattamento dei dati personali
- Design e Default: la necessità dei titolari del trattamento dei dati di adottare misure tecniche ed organizzative che dimostrano il rispetto dei principi fondamentali GDPR

Gli strumenti proposti da IBM sono in grado di ricercare i dati sensibili nelle piattaforme aziendali e cloud, identificarli, mascherarne la lettura ed interpretazione, gestirne il ciclo di vita supportando l'analisi dei flussi di gestione del dato attraverso l'adozione, quando necessaria, di componenti quali StoredIQ, CaseManager, la suite Infosphere ed Optim.

La Sicurezza del Dato richiesta dalla legge è supportata da un primo livello di applicazioni (Compliance Monitoring &Enforcing) che si occupano del far rispettare le politiche di sicurezza del dato nei sistemi aziendali (Guardium), verificare

le vulnerabilità delle applicazioni che gestiscono il dato (Appscan) e quindi mantenere un continuo controllo sulla sicurezza aziendale (Qradar) che consente di rilevare le eventuali violazioni al momento in cui si manifestano ed organizzare i processi di gestione di un eventuale incidente (Resilient System).

Per garantire la sicurezza questo nucleo di tecnologie avrà bisogno del supporto di soluzioni per la protezione della infrastruttura IT aziendale (Organic Infrastructure Protection) che dovranno occuparsi della gestione delle Identità e dell'accesso ai sistemi aziendali da parte degli utenti (Suite IBM Security IAM), controllare l'accesso degli utenti ad applicazioni adottate dalla Azienda in Cloud (IBM Cloud Security Enforcer), proteggere e gestire gli Endpoint Mobile (MaaS360) e tradizionali (BigFix) nonché proteggere le reti aziendali (IBM Network Protection XGS).

Le tecnologie IBM sono collaborative con centinaia di ulteriori soluzioni applicative e di sicurezza informatica e possono aiutare l'Azienda ad ottenere il livello di controllo del rispetto della normativa.

Un ventaglio di soluzioni a supporto della compliance: **due esempi**

1 QRadar

Tra le diverse componenti di sicurezza che possono essere attivate in maniera collaborativa per aiutare una azienda nella compliance con la GDPR, c'è QRadar.

IBM QRadar Security Intelligence può aiutare, se correttamente utilizzato e configurato nel sistema di protezione, a monitorare continuativamente gli eventi log, le identità di chi accede ai sistemi, le vulnerabilità presenti, i flussi di comunicazione all'interno del sistema informativo.

Collaborando con le altre componenti di sicurezza perimetrale o dell'Endpoint, si potrà occupare di verificare comportamenti malevoli e di supportare la individuazione di eventuali violazioni supportando la verifica della compliance con i requisiti di legge fornendo report sulle attività del sistema informativo.

QRadar può identificare minacce ad alto rischio, attacchi e violazioni della sicurezza tramite la correlazione in tempo reale utilizzando la QRadar Sense Analitics, quindi mettere in alta priorità gli incidenti rispetto a miliardi di eventi ricevuti giornalmente.

Una volta rilevata una attività malevola può collaborare con sistemi di sicurezza che consentano il blocco del traffico di rete e/o altre attività di reazione all'attività illecita oltre a creare la prima evidenza della violazione che potrà essere inviata ad ad una piattaforma di gestione dell'incidente.

Nel viaggio verso la protezione del dato sensibile secondo la normativa GDPR, QRadar ricopre una fondamentale funzione per la messa in evidenza di eventuali anomalie, centrale rispetto alla necessaria capacità di controllo continuo delle attività dei sistemi informativi.

2 InfoSphere

IBM InfoSphere Optim Data Privacy codifica on demand le informazioni riservate dell'intera azienda, incluse le piattaforme big data. La soluzione codifica i dati di applicazioni, database e report degli ambienti di produzione e non, sia in modo statico che dinamico. InfoSphere Optim Data Privacy migliora la protezione dei dati e supporta le iniziative di conformità.
Consente inoltre alle aziende di:
Codificare on demand i dati riservati di applicazioni, database e report in base alle policy di business per proteggere la privacy dei dati.

- Supportare le iniziative di conformità dell'intera azienda.
- Codificare i dati riservati in modo dinamico in ambienti big data e sul cloud.
- Applicare una serie di tecniche di data masking per trasformare le informazioni personali codificate e altri dati aziendali riservati.
- Trarre vantaggio dalle routine di data masking preintegrate per trasformare i dati complessi, come numeri delle carte di credito, indirizzi e-mail e ID nazionali, mantenendo il significato contestuale.
- Consolidare e codificare i dati di più applicazioni in correlazione per creare un ambiente di test di produzione simulato che riflette accuratamente i processi di business. Migliorare la conformità con normative sulla privacy, come Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), i requisiti Digital Due Process (DDP), Personal Information Protection and Electronic Documents Act (PIPEDA), i requisiti Safe Harbor e Payment Card Industry Data Security Standard (PCI DSS).Utilizzare un'unica soluzione di data masking enterprise scalabile per codificare i dati di applicazioni, database e sistemi operativi.Codificare on demand i dati riservati di applicazioni, database e report.
- Supportare le iniziative di conformità uniformi.
- Migliorare la conformità con normative sulla privacy, come Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), i requisiti Digital Due Process (DDP), Personal Information Protection and Electronic Documents Act (PIPEDA), i requisiti Safe Harbor e Payment Card Industry Data Security Standard (PCI DSS).
- Utilizzare un'unica soluzione di data masking enterprise scalabile.
- Si integra con le applicazioni più utilizzate, come Oracle E-Business Suite, PeopleSoft Enterprise, Siebel, JD Edwards EnterpriseOne, SAP e Amdocs CRM.
- Può essere utilizzato con le tecnologie di database IBM DB2, IMS, Virtual Storage Access Method/Sequential (VSAM/SEQ), Adabase, Informix, Oracle, Sybase, SQL Server e XML.
- Compatibile con i sistemi operativi Microsoft Windows, Unix, Linux e IBM z/OS.


S.I.P.E.
SOLUZIONI INFORMATICHE PERSONALIZZATE
www.sipe.it
IBM
Gold
Business Partner
12