...making excellence a habit.

Il Regolamento Europeo per la Data Protection

Scenario e approfondimenti

Whitepaper

In sintesi

La European Data Protection Directive 95/46/EC nasce come evoluzione dell'Irish Data Protection Act 1988 e 2003. La direttiva definisce un nuovo equilibrio tra i diritti umani e le necessità organizzative, fornendo un framework per la gestione equa e conforme dei dati.

Il 21 ottobre 2013, le Associazioni per le Libertà Civili hanno votato per la definizione di una riforma che ha portato alla moderna Direttiva per la Data Protection, con l'obiettivo di ridare agli utenti il controllo sui propri dati personali, promuovere la fiducia nei social media e nello shopping online e accrescere la protezione dei dati personali gestiti da polizia e autorità giudiziarie.

In seguito a diversi anni di dibattiti e discussioni sulle normative proposte, il 14 aprile 2016 il Parlamento Europeo ha dato l'approvazione finale alla delibera della normativa UE per la Data Protection, entrata in vigore dopo 20 giorni.

La normativa si applica unilateralmente in tutti gli Stati Membri dell'Unione Europea entro 2 anni dalla pubblicazione, che avrà valore esecutivo a partire dal 25 maggio 2018.

Le implicazioni per le organizzazioni sono estremamente rilevanti. Il presente documento approfondisce la natura e lo scopo delle riforme in piano, le considerevoli sfide che rappresentano per il business e il modo migliore per approcciarle. È di particolare rilevanza sia per i professionisti della conformità e della sicurezza dei dati, che per i responsabili Sales, Marketing e Risorse Umane.

Scenario

Perché una riforma UE per la protezione dei dati

In origine, la Data Protection Directive del 1995 è stata interpretata e recepita in modo diverso tra le diverse nazioni dell'UE, causando differenze significative nell'applicazione della direttiva, sia tra i diversi Stati Membri che all'interno della stessa nazione.

Molto è cambiato dal 1995: smartphone e tablet sono ora onnipresenti e l'utilizzo di dispositivi mobili e l'accesso a internet da qualsiasi dispositivo lasciano una traccia digitale, che può essere ricondotta ad un individuo. L'affermazione dei social media e la proliferazione di app che tracciano ogni dettaglio delle nostre vite digitali, ha richiesto la definizione di una normativa globale per la data protection.

Gli obiettivi della riforma

La Direttiva per la Protezione dei Dati ha 5 obiettivi che possono essere sintetizzati come segue:

- Rinforzare il rispetto dei diritti umani - privacy by design e by default
- Fortificare il mercato interno dell'UE attraverso nuove regole chiare e robuste per la libera circolazione di dati
- Garantire l'entrata in vigore di regole chiare e coerenti
- Definire standard globali di data protection
- Garantire un alto livello di data protection in tutte le organizzazioni

I pilastri della riforma UE

La Commissione Europea fa riferimento ai 4 "pilastri" della normativa:

Pilastro 1: un continente, una sola legge regolamentata da sanzioni

La Direttiva si applica uniformemente a tutti gli Stati Membri dell'UE senza la necessità di implementare delle normative nazionali per recepirla. Queste sono le implicazioni:

- Armonizzazione della legislazione all'interno del mercato europeo
- Parità di condizioni per il business attraverso un'unica legge applicabile a qualsiasi azienda nell'UE
- Risparmio stimato per il business fino a €2,3 miliardi all'anno.

Verranno applicate significative sanzioni in seguito alla violazione della direttiva. Di seguito, i casi presentati in due livelli:

- Livello 1 – Fino a €10 milioni o fino al 2% del fatturato mondiale annuale

Questo livello viene applicato nel caso di violazioni alla normativa in cui, per esempio, non venga definito un contratto scritto tra chi controlla e chi processa i dati.

È ora responsabilità delle organizzazioni che processano e controllano dati personali e sensibili di avere un contratto scritto chiaro e conciso nel caso di cessione a una parte terza (un Processore di Dati).

- Livello 2 – Fino a €20 milioni o fino al 4% del fatturato mondiale annuale

Questo livello si applica nei casi in cui, ad esempio, un'azienda non ottenga un esplicito consenso dall'utente per la gestione dei dati personali sensibili.

Pilastro 2: Le aziende non europee dovranno sottostare alla Direttiva Europea per la Data Protection se operano nel mercato europeo.

Questo si applica sul territorio come segue:

- La normativa si applica alle organizzazioni fuori UE
- Lo stesso vale per le organizzazioni fuori dall'UE che processano dati personali insieme alla fornitura di servizi per o al monitoraggio di individui localizzati nell'UE
- Gli individui hanno il diritto di fare riferimento alla propria autorità nazionale per la protezione dei dati, anche se i dati sono processati al di fuori del proprio Paese

Pilastro 3: Diritto all'oblio / cancellazione

Quando un individuo desidera che i propri dati non vengano più processati, e non sussiste alcuna ragione legittima per mantenerli, i dati devono essere cancellati. Questo per dare potere agli individui, e non per cancellare eventi passati o ostacolare la libertà di stampa. In particolare:

- Il "diritto all'oblio" viene ora definito "diritto di cancellazione"
- L'onere di provare che sussiste necessità di mantenere i dati è a carico di chi controlla i dati, non dell'utente

Alcune spiegazioni:

- Nel caso in cui una particolare tecnologia non ne consenta la cancellazione, all'utente può essere concesso di avere una "restrizione" per i propri dati.
- Per rinforzare il diritto all'oblio ogni individuo ha diritto di non essere profilato
- Profilazione = qualsiasi forma di controllo automatizzato dei dati personali inteso a valutare certi aspetti personali legati ad una persona naturale o per analizzare o predire le performance di una persona naturale riguardo a lavoro, situazione economica, posizione, salute, preferenze personali, affidabilità o comportamento

Pilastro 4: Modalità "one-stop-shop" per aziende e cittadini

È stato discusso il concetto di one-stop shop. L'idea è che le organizzazioni possano avere una singola autorità di supervisione/regolatoria a sovraintendere le attività di gestione dei propri dati in tutti gli Stati Membri UE. Ad ogni modo:

- È possibile che sia necessaria una "lead authority" perché si consulti con tutte le altre autorità competenti
- È possibile che questo punto venga ulteriormente discusso per fare maggiore chiarezza sui requisiti specifici di supervisione

Cosa comporta per gli individui

L'obiettivo primario delle riforme per la data protection è quello di rafforzare i diritti dei cittadini. La presenza di norme più restrittive per la data protection rafforzeranno il controllo degli individui sui propri dati personali. Gli elementi seguenti verranno significativamente migliorati:

- **Libero consenso dichiarato**
  L'obbligo di dichiarazione del consenso per la gestione dei dati personali, fornisce all'utente il controllo su di essi, poiché il consenso deve essere esplicito. Non può essere sottinteso. Le organizzazioni hanno inoltre l'obbligo di informare tempestivamente il soggetto riguardo a violazioni interne di dati che possano riguardarli
- **Accesso semplificato ai dati personali**
  Il diritto alla portabilità dei dati rende più semplice per il soggetto trasferire i propri dati da un fornitore di servizi ad un altro
- **Divulgazione alle autorità di terza parte**
  Gli utenti hanno il diritto di sapere se i propri dati sono stati forniti su richiesta ad una pubblica autorità. Tale trasferimento di dati personali richiesto dai tribunali nazionali o da un'autorità amministrativa sarà (per la maggior parte) proibito.

  Questo cambierà le eccezioni ai trasferimenti di dati frequenti o su larga scala e all'uso di traffico e localizzazione da parte delle autorità pubbliche ai fini della sicurezza nazionale e delle attività legislative

- **'Privacy by design' e 'privacy by default'**
  Si tratta di principi chiave per la protezione dei dati nel nuovo regolamento UE. Significa che le procedure di data protection devono essere incorporate all'interno di prodotti e servizi sin dai primi stadi dello sviluppo, e che devono essere definite impostazioni "privacy-friendly" in ogni ambito – ad esempio per i social network.

Le impostazioni di privacy sono definite ad alti livello "by default". Le verifiche (Data protection Impact Assessment - Articolo 33), devono essere realizzate nei casi in cui sussistono specifici rischi per i diritti e la libertà degli utenti. La valutazione e il controllo dei rischi è ora un requisito e nel caso di situazioni ad alto rischio richiede l'approvazione preventiva del DPA.

Le sfide per le organizzazioni

Sono numerose le sfide che le organizzazioni si devono preparare ad affrontare fin da ora.

Notifica mandatoria della violazione dei dati

- Attualmente le condizioni secondo cui una violazione debba essere notificata non sono definite in modo chiaro
- Il nuovo regolamento sancisce la notifica mandatoria ai soggetti proprietari dei dati e alle autorità competenti
- Questo può comportare la necessità di inoltrare la notifica entro 72 ore

Per qualsiasi azienda, abbastanza sfortunata da subire una violazione dei dati che si trovi in una situazione di crisi e, contemporaneamente, a dover fornire una notifica dettagliata ai clienti coinvolti (o persino agli organismi di controllo), rappresenta indubbiamente una sfida. Quando questo si combina a processi di incident responce, insieme all'identificazione delle cause della violazione, ai tentativi di gestione della vulnerabilità e alla valutazione dell'estensione dei danni, il processo diventa esponenzialmente più complesso.

L'obbligo di segnalare la violazione dei dati entro 72 ore rappresenta una sfida enorme per le organizzazioni. In mancanza di piani e procedure di risposta alle minacce/violazioni, risulta impossibile per le organizzazioni effettuare la notifica secondo i nuovi termini normativi.

Nomina mandatoria d un Data Protection Officer

Le organizzazioni dovranno nominare un Data Protection Officer (DPO) designato se le attività core coinvolgono il regolare e sistematico monitoraggio o la gestione dei dati del tipo:

- Dati sensibili, inclusi biometrici o genetici
- Dati relativi a condanne o informazioni penali

Inoltre, qualsiasi ente o autorità pubblica dovrà nominare un DPO. Nelle circostanze sopra citate, devono sussistere le seguenti condizioni nel processo di nomina per tale posizione:

- Il Data Protection Officer deve dimostrare le poprie competenze professionali ed esperienze
- Il Data Protection Officer deve essere designato per un periodo minimo prestabilito e deve avere un livello minimo di qualifiche definito
- Il DPO deve essere indipendente
- Il controllo del DPO è responsabilità del Regolatore e non del Board

La nomina di una figura idonea qualificata e competente rappresenta una sfida per la maggior parte delle organizzazioni.

Attualmente, la lista di professionisti con esperienza in ambito data protection è molto limitata. Persino gli esperti attualmente impiegati in quest'area potrebbero non avere le certificazioni necessarie per rispondere ai requisiti normativi richiesti.

Molte organizzazioni potrebbero pensare di eligere un membro dello staff già impiegato per ricoprire tale ruolo. Ad ogni modo, il DPO deve dimostrare il suo stato indipendente dall'organizzazione ("in the company", ma non "of the company"), e dovrà rispondere esternamente alla Lead Authority. La gestione di ogni situazione percepita come conflitto di interessi risulterà complessa.

Di conseguenza, ci si aspetta che le organizzazioni preferiranno un modello outsourced per indirizzare le casistiche sopra citate.

L'impatto delle sanzioni

Il crescente impatto delle sanzioni monetarie e la frequenza con cui ci si aspetta che verranno applicate, rappresenta una preoccupazione non indifferente per la maggior parte delle organizzazioni.

Sebbene il costo dell'implementazione di misure di data protection/privacy possa costituire un importante esborso per le organizzazioni, di contro va considerato come un investimento giustificabile per prevenire eventuali costi e danni dovuti all'assenza di tali misure o nell'eventualità di una violazione di dati.

Costi iniziali

Alcuni dei nuovi requisiti richiedono alle organizzazioni di adeguare e allineare i propri processi. L'impatto di tale operazione rappresenta un costo in termini di:

- Cambiamenti alle modalità di acquisizione del consenso esplicito per la gestione dei dati a tutti i livelli di business, in particolare per quelle aziende che gestiscono attività di direct marketing oppure hanno necessità di mantenere contatti duraturi nel tempo con i propri clienti
- Le misure tecniche per garantire che il consenso sia ottenuto in modo esplicito richiederanno costi di sviluppo. Ad esempio, aggiornare moduli web-based, pop-up cookie e e-mail marketing richiederà tempi e costi di sviluppo perché siano adeguati nel rispetto della normativa
- Le organizzazioni che si affidano all'analisi dei dati personali, al tracking o al monitoraggio delle attività degli utenti, nel peggiore dei casi potrebbero trovarsi a perdere informazioni importanti per la profilazione dei dati nel caso di un mancato consenso esplicito. In tal caso, il modello di business andrà rivisto per rimanere sostenibile
- Per garantire misure idonee alla nuova portabilità dei dati, alcune organizzazioni avranno bisogno di cambiare drasticamente il proprio approccio alla gestione dei dati e garantire che la richiesta di trasferimento o di movimento venga accolta tempestivamente
- Rispondere alle richieste degli utenti in materia di protezione dei dati può richiedere tempo e denaro. Il processo secondo cui i soggetti possono effettuare una richiesta di cancellazione/modifica dei propri dati verrà semplificato. Le organizzazioni potranno avere un aumento di richieste conseguenti alla normativa, che esigerà la messa a punto di procedure e coinvolgerà le risorse dell'organizzazione
- Nel caso in cui un utente faccia appello al diritto di cancellazione dei propri dati, l'organizzazione deve dimostrare chiaramente e senza ombra di dubbio di aver fatto fronte alla richiesta. Garantire la rimozione da tutti i sistemi di tutta l'organizzazione dei dati personali, può rappresentare nel tempo un costo per l'organizzazione.

Implementazione

Per tutte le organizzazioni che devono adeguarsi ai requisiti della normativa in materia di data protection, il modo migliore per prepararsi è implementare una solida strategia di data protection e processi che idealmente includano best practice per i controlli di sicurezza.

I nostri specialisti in materia di data protection hanno una profonda conoscenza ed esperienza nella pianificazione, realizzazione e mantenimento di programmi di Data Protection in diversi ambiti industriali. In qualità di esperti, siamo in grado di supportarti nella scelta e definizione delle migliori pratiche per il controllo della sicurezza e il mantenimento conforme dei tuoi dati.

La normativa in materia di data protection e privacy non richiede alcun tipo di controllo tecnico specifico. Ad ogni modo, la migliore pratica è l'implementazione nel cuore del business di controlli tecnici per rendere i dati personali non accessibili agli utenti non espressamente autorizzati alla loro gestione. I controlli possono includere:

- Meccanismi di controllo dell'accesso degli utenti
- Crittaggio
- Oscurare i dati nei casi in cui l'accesso non è richiesto

Il nostro team di consulenti esperti lavora con le organizzazioni fornendo informazioni e soluzioni utili in diversi ambiti della data protection. I servizi includono:

- Supporto all'implementazione della data protection
- Sevizi di Data Protection Officer (onsite e/o virtuale)
- Data protection /privacy impact assessment
- Corsi di formazione
- Supporto per i data protection audit (interni e/o esterni)
- Supporto nella preparazione degli accessi per gli utenti

Benefici

C'è da considerare il fatto che la normativa in materia di privacy e data protection non rappresenta solamente un elemento negativo per le organizzazioni. Sebbene non siano particolarmente evidenti, sono molti i benefici nel raggiungimento della conformità alla nuova normativa.

Ridurre le probabilità di rischio di una violazione dei dati, significa evitare le sanzioni associate alla non conformità alla normativa.

- Vengono evitati i danni alla reputazione e la cattiva pubblicità
- Vengono definiti processi customer focused e rigore nella governance degli stakeholder
- Garanzia per clienti e normatori che le best practice sono applicate
- Privacy impact assessment per identificare i problemi fin dai primi stadi della progettazione e ridurre così l'impatto sul business

L'applicazione dei requisiti normativi può rappresentare un'opportunità per ridisegnare i processi di business. L'organizzazione potrebbe cogliere l'opportunità per ridurre i costi minimizzando, dove possibile, la mole di informazioni immagazzinate, migliorando la trasparenza dei processi per tutti i dipendenti.

Mercato di riferimento

Il presente documento è rilevante e porta benefici a chiunque sia coinvolto nelle fasi di trattamento, archiviazione e gestione delle informazioni personali. Questo include:

- Data Protection Officer
- Human Resource Manager
- Sales and Marketing Manager
- Information Security Professional
- Compliance and Audit Manager
- Healthcare Professional

Conclusioni

Comprendiamo il valore dei dati per la tua organizzazione e le gravi implicazioni della violazione dei dati. Aiutiamo le imprese ad applicare best practice per la gestione e il mantenimento della conformità agli standard del regolamento UE. Raccomandiamo un approccio risk-based per promuovere l'uso e la gestione responsabile dei dati.

In sintesi, se vuoi prepararti alla nuova normativa in materia di Data Protection, è necessario che la tua organizzazione cominci fin da subito a sviluppare e implementare un programma di data protection.

Informazioni aggiuntive

- **Q&A European Data Protection Reform**
  http://www.europarl.europa.eu/news/en/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform
- **Commissione Europea – Data Protection**
  http://ec.europa.eu/justice/data-protection/index_en.htm
- **Il cliente al centro dell'attenzione: più libertà, più diritti, più scelta**
  http://ec.europa.eu/commission/2014-2019/jourova/announcements/putting-consumer-centre-more-freedom-more-rights-more-choice

Cybersecurity e Information Resilience

I nostri servizi in ambito Cybersecurity e Information Resilience consentono alle organizzazioni di mettere in sicurezza le informazioni dagli attacchi informatici, rafforzare l'Information Governance e mitigare i rischi agendo sulle vulnerabilità dell'infrastruttura critica. Aiutiamo le organizzazioni a gestire le sfide nell'ambito della sicurezza delle informazioni:

Consulenza

Cybersecurity e information resilience, security testing e supporto specialistico

Formazione

Corsi di formazione specialistici per la crescita professionale

Ricerca

Ricerche di mercato e progetti di horizon scanning

Soluzioni tecniche

Soluzioni cloud per supportare la tua organizzazione

Our expertise is supported by:

CREST · PCI Security Standards Council QUALIFIED SECURITY ASSESSOR · CYBER ESSENTIALS · CSA cloud security alliance SM

Scopri di più

T: +39 02 6679091
E: marketing.italy@bsigroup.com
W: bsigroup.it