CYBER RISK
ASSESSMENT & MNGT
Inquadramento e gestione del rischio, data breach, profili di responsabilità.
Cosa cambia alla luce del
Regolamento Generale europeo sul trattamento dei dati personali 2016/679

Inquadramento del rischio e profili di responsabilità

Avvocato Marco Maglio

Milano, 3 novembre 2016

Via Gardella, 2 Sala Ruffini presso la sede di Vittoria Assicurazioni S.p.A.

Cosa cambia

- La nuova privacy:

- caratteristiche, tempi ed ambito di applicazione

- Le nuove parole chiave:

- Accountability, Privacy by design e Privacy by default

- I nuovi ruoli del trattamento:

- cosa cambia per il titolare
- cosa cambia per il responsabile (e gli incaricati)
- il Data Protection Officer

Cosa cambia

-- I nuovi diritti:

- cosa cambia per l'interessato con il diritto all'oblio e il diritto alla portabilità dei dati

- I nuovi adempimenti in tema di sicurezza:

- sparisce la notificazione ma nasce il registro dei trattamenti
- il Privacy Impact Assessment
- come cambiano informativa e consenso
- misure di sicurezza e data breach notification

- Le nuove opportunità per i titolari del trattamento

- privacy seal e certificazioni di conformità

- Le nuove sanzioni:

- come cambiano e chi le applicherà

Seconda parte – cosa bisogna fare

- **La privacy come processo aziendale:**

- cosa significa in concreto

- **Le nuove best practice:**

- diffondere la cultura del dato in azienda,
- creare un gruppo di lavoro per definire i criteri di trattamento dei dati,
- prevedere un privacy program e mappare i dati aziendali
- definire il ciclo di vita dei dati personali
- creare una data policy retention
- realizzare una valutazione d'impatto del trattamento dei dati aziendali e fare l'analisi dei rischi

- **Lo scenario futuro:**

- i privacy management tools e la scatola nera del trattamento dei dati.

Come cambiano gli attacchi informatici

Dalla prima pagina del Corriere della sera del 23 ottobre 2016

CORRIERE DELLA SERA

Il cyber attacco contro Internet negli Usa partito dalle case «intelligenti»

L'attacco è arrivato da oggetti «smart»: videoregistratori, frigoriferi, telecamere di sicurezza, router e sistemi per il controllo dei neonati.

Si tratta di oggetti sempre più diffusi —oggi se ne contano 7 miliardi nel mondo, nel 2020 saranno quasi 30 — e rappresentano forse il più grande problema di sicurezza informatica del momento, perché vulnerabili adattacchi esterni

La regola base per tutelare i dati personali

Per garantire la tutela dei dati personali è da tempo previsto questo meccanismo di tutela giuridica:

1) i dati personali sono tutte le informazioni che sono riconducibili ad una persona

2) per poter raccogliere ed usare questi dati occorre:
   - informare la persona cui si riferiscono i dati;
   - raccogliere il suo consenso espresso, libero, informato e specifico (salvo eccezioni).

Questo vale sia per i dati comuni che per i dati sensibili.

L'applicazione di questa regola ha subito nel corso del tempo un'evoluzione rappresentata da tre tappe essenziali.

Le tre tappe della tutela dei dati personali

1. **Direttiva comunitaria 95/46/CE**

1. **Direttive Comunitarie 2002/58/CE** e **2009/136/UE**

1. **Regolamento europeo 2016/679 che abroga la direttiva 95/46**

Le tre tappe della tutela dei dati personali

1) La **Direttiva comunitaria 95/46/CE** ha fissato i principi generali della normativa in materia di dati personali per consentire la libera circolazione dei dati personali nel territorio europeo.

1) Le **Direttive Comunitarie 2002/58/CE** e **2009/136/UE** relative al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche hanno introdotto alcune precisazioni specifiche rispetto alla Direttiva 95/46 che riguardano la raccolta di dati personali effettuata on line e in particolare all'uso dei cookies.

1) il **Regolamento (UE) 2016/679** del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

Tempi di recepimento

Il regolamento è stato pubblicato il **4 maggio 2016,** ed è **in vigore dal 25 maggio 2016.**

Diventa pienamente operativo due anni dopo la sua pubblicazione in Gazzetta Ufficiale dell'Unione Europea quindi il **25 maggio 2018**.

Si tratta di un testo normativo ad efficacia differita per permettere l'armonizzazione tra i vari ordinamenti nazionali interessati. Tuttavia ben prima del 2018 il nuovo testo farà sentire i suoi effetti. I Garanti nazionali favoriranno l'armonizzazione tra gli stati anticipando parti significative della riforma.

Le principali novità per l'Italia

In Italia i campi di maggiore rilevanza e novità sono:

- Obbligo di definire i tempi di conservazione dei dati.
- Obbligo di indicare la provenienza dei dati in caso di utilizzo.
- Obbligo di comunicare tempestivamente al Garante violazioni dei propri database.
- Obbligo di predisporre il documento di valutazione di impatto del trattamento dei dati personali.
- Obbligo di gestire *l'accountability* in materia di data protection con adeguati presidi organizzativi (prevalentemente mediante il Data Privacy Officer).

Cosa cambia per le infrastrutture di sicurezza

I nuovi imperativi:

1) Tratta meno dati che puoi

2) Distribuisci le responsabilità e documenta i trattamenti

3) Favorisci l’anonimizzazione e la pseudonimizzazione

4) Gestisci la privacy by default e by design

5) Introduci l’accountability nella gestione dei ruoli del trattamento dei dati

L’impatto del regolamento sulle imprese

Il Regolamento pur con molte mediazioni **stabilisce nuovi diritti sul trattamento dei dati personal**i:

- Introduce nuove regole organizzative per il corretto trattamento dei dati personali. Tuttavia il consenso non deve essere più espresso;
- definisce sanzioni pesanti e commisurate al fatturato delle aziende;
- crea meccanismi di tracciabilità che imporranno alle aziende di allocare al loro interno le responsabilità nel trattamento dei dati personali.

L’impatto del regolamento sulle imprese

La gestione dei dati personali non è più solo un **adempimento**, ma diventa un **processo aziendale** che incide sull’organizzazione delle imprese.

Per gestire al meglio questo passaggio ci sono alcune cose essenziali da sapere.

caratteristiche, tempi ed ambito di applicazione

Le norme interesseranno **tutti quei soggetti (anche extraeuropei)** che sono **chiamati a trattare** (in maniera automatizzata o meno) **i dati**.

In sostanza, viene introdotto il principio dell'applicazione del diritto dell'Unione Europea anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni o servizi a cittadini UE o tali da comportare il monitoraggio dei loro comportamenti.

A chi si applica la normativa

È una **rivoluzione** rispetto alla regola precedente in base alla quale la normativa applicabile è quella del luogo in cui ha sede il Titolare del trattamento.

Social network, piattaforme web e motori di ricerca saranno soggette alla normativa europea anche se gestite da società con sede fuori dall'Unione Europea.

E' rilevante anche per quanto riguarda i servizi gestiti in modalità cloud

Le nuove regole di sicurezza

Il caposaldo del sistema di sicurezza del regolamento europeo è definito dall' articolo 32 «Sicurezza del trattamento» che prevede quanto segue

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Le nuove regole di sicurezza

Articolo 32

Sicurezza del trattamento

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei 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.

3. L'adesione a un codice di condotta o a un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare la conformità ai requisiti di sicurezza.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Viene anche prevista la necessità di una consultazione preventiva dell'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

Le nuove parole chiave

Dovere di documentazione e di informazione

Sarà necessario **elaborare un sistema documentale di gestione della privacy** contenente tutti gli atti, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità al Regolamento.

Viene introdotto l'obbligo di **istituire un registro del trattamenti dei dati**.

Tutte le operazioni di trattamento devono essere tracciabili e documentabili.

È la logica della «scatola nera».

Le nuove parole chiave

Dovere di documentazione e di informazione: accountability

È l'applicazione operativa del **principio di rendicontazione e responsabilità** (o di "**accountability**"), secondo cui il Titolare del trattamento deve conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità.

Occorre indicare per ognuno di essi, una serie di informazioni, tali da assicurare e comprovare la conformità di ciascuna operazione alle disposizioni del Regolamento (qualcosa di simile al Documento Programmatico sulla Sicurezza, ma di portata più ampia).

Si chiede di effettuare un'adeguata analisi dei rischi e documentarla.

Le nuove
parole chiave

Privacy by design e Privacy by default

I Titolari del trattamento dovranno, pertanto, prevedere meccanismi di protezione dei dati fin dalla progettazione delle attività e per l'intera gestione del ciclo di vita dei dati - dalla raccolta alla cancellazione - incentrandosi sistematicamente sulle garanzie procedurali in merito all'esattezza, alla riservatezza, all'integrità, alla sicurezza fisica ed alla cancellazione dei dati.

Le nuove parole chiave

Privacy by design e Privacy by default

Si tratta dell'esplicitazione del **principio dell'incorporazione della privacy fin dalla progettazione del processo aziendale** e degli applicativi informatici di supporto, ovvero la messa in atto di meccanismi per garantire che siano trattati - di default - solo i dati personali necessari per ciascuna finalità specifica del trattamento.

Significa in pratica che occorre programmare e progettare i trattamenti di dati personali e prevenire possibili rischi nel trattamento ed abusi nell'utilizzo di tali informazioni.

Le nuove parole chiave

Privacy by design e Privacy by default

L’articolo 25 del Regolamento prevede la protezione per impostazione predefinita

«Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per

- la quantità dei dati personali raccolti,
- la portata del trattamento,
- il periodo di conservazione
- l’accessibilità.

In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l’intervento della persona fisica.

Le nuove responsabilità del Titolare

Il testo dell'articolo 24 del Regolamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, **il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente** al regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure adottate includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

3. L'adesione ai codici di condotta o a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Le nuove responsabilità del responsabile

Il testo dell'articolo 28 del Regolamento

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Designazione di un Data Protection Officer

Il Regolamento introduce la figura **del "Responsabile per la protezione dei dati" o Data Privacy Officer (DPO)**. Non è un semplice responsabile del trattamento, è il **manager del trattamento dei dati**.

Si tratta di una nuova figura professionale che deve idealmente possedere o acquisire competenze ampie (giuridiche, informatiche, organizzative) e svolgere un'attività che non è di mero controllo formale ma di supporto strategico alle decisioni operative del Titolare.

È il **privacy designer**, il progettista della sicurezza nel trattamento dei dati.

Designazione di un Data Protection Officer

Le categorie che dovranno nominarlo sono

- Tutte le **autorità** ed **organismi pubblici**
- Le **imprese che trattino i dati di un rilevante numero di persone** (c.d. interessati) **o tipologie di dati** che per natura, oggetto o finalità siano definite categorie **"a rischio"** dalla normativa.

Designazione di un Data Protection Officer

Il DPO deve essere designato come soggetto referente del Garante e opera con ampia autonomia e competenza professionale.

Può essere un soggetto interno o esterno e il suo mandato, revocabile e rinnovabile, dura quattro anni.

I nuovi adempimenti

Valutazione d’impatto sulla protezione dei dati

I Titolari dovranno effettuare una Valutazione degli impatti privacy (**Privacy Impact Assessment – PIA**) fin dal momento della progettazione del processo aziendale e degli applicativi informatici di supporto, nei casi in cui il trattamento alla base degli stessi, per sua natura, oggetto o finalità, presenti rischi specifici per i diritti e le libertà degli interessati.

I nuovi adempimenti

Valutazione d’impatto sulla protezione dei dati

Il PIA andrà realizzato per trattamenti potenzialmente rischiosi.

Occorrerà:

1. **Condurre l’analisi dei rischi**
2. **Definire i Gap rispetto alla corretta gestione dei rischi**
3. **Stabilire un Action Plan per colmare questi Gap**
4. **Controllare annualmente gli interventi effettuati per ridurre i rischi**

I nuovi adempimenti

Obblighi di segnalazione in caso di violazione sui dati

I Titolari del trattamento, in caso di una violazione dovranno mettere in atto due differenti azioni:

- la notificazione della violazione all'Autorità di controllo entro 72 ore dal fatto;
- la segnalazione al diretto interessato (senza ritardo ingiustificato) qualora la violazione possa comportare dei danni per l'interessato stesso.

Sarà l'Autorità Garante locale a valutare la necessità di informare i singoli interessati i cui dati siano stati oggetto di violazione

Le nuove opportunità

Privacy seal e certificazioni

Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

La certificazione è volontaria e accessibile tramite una procedura trasparente.

La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti

Le nuove opportunità

Privacy seal e certificazioni: La Roadmap

In questa fase i Titolari possono iniziare il percorso preparatorio alla certificazione sottoponendosi a assessment ed effettuando audit specifici sulla base dei protocolli di certificazione già esistenti.

a) il protocollo BSI:10012

Gestione delle informazioni personali

Realizza processi e operazioni per la corretta gestione della privacy

b) il protocollo EuroPriSe

European Privacy Seal

basato sulla direttiva 95/46

Questo è il percorso intrapreso da IDMC che nel 2016 si è sottoposta a certificazione volontaria sulla base del protocollo EuroPriSe e BSI

Aumentano le sanzioni

Diventano molto più pesanti e vengono applicate dai Garanti in stretto coordinamento tra loro :

- Fino a **€ 20.000.000** per i privati e le imprese non facenti parte di gruppi.
- Fino al 4% del fatturato complessivo (consolidato) per i Gruppi societari.

Si tratta di un cambio di passo significativo. Le sanzioni sono pensate per incidere sulle condotte dei grandi gruppi multinazionali che trattano dati in diverse aree geografiche e spesso cercano di individuare i paradisi legali del trattamento dei dati personali per eludere norme e criteri di comportamento definiti dalle nazioni più rigorose.

Cosa bisogna fare?
Definire un privacy program

Per le organizzazioni che trattano dati personali in modo significativo diventa essenziale definire un piano di azione per gestire in modo adeguato le regole che sono introdotte dal Regolamento Europeo:

occorre definire un **Privacy Program**

Questi sono i passi preliminari da intraprendere:

1) Fare un inventario delle proprie informative e verificare come potrebbero cambiare in funzione delle nuove regole. Valutare cosa significa in concreto dover introdurre l'indicazione della fonte dei dati e il tempo di conservazione dei dati.
2) Sperimentare nuove forme di informative visuali basate su icone.

Cosa bisogna fare?
Definire un privacy program

3) Analizzare quali sono i dati di cui si dispone e fare una mappatura aggiornata dei dati.
4) Dotarsi di “software sentinella” per gestire il nuovo obbligo di notifica delle violazioni nell’uso dei dati personali e verificare l’eventuale flusso extraeuropeo dei dati usando servizi cloud.
5) Sperimentare la Privacy by Design e effettuare il Privacy Impact Assessment affidandosi a esperti competenti che aiutino l’azienda a minimizzare gli impatti e a contenere i costi di gestione dei nuovi adempimenti.
6) Pensare a come introdurre un Data Protection Officer in azienda.

Cosa bisogna fare?
Definire un privacy program

7) Analizzare gli effetti del diritto alla portabilità dei dati e adottare cautele organizzative per evitare impatti gravi sulla stabilità dei data base aziendali.
8) Definire le nuove regole di acquisizione e documentazione del consenso.
9) Verificare con cura i fornitori dei dati. Questo è il tempo in cui fare test, test e ancora test.
10) Verificare se si trattano dati di minori tenendo conto che le nuove regole impongono di gestire anche il consenso degli esercenti la potestà di genitore con il consenso del minore al di sotto dei 16 anni.

E non finisce qui…

La **data protection** sarà sempre di più un **fattore competitivo e favorirà le aziende che capiranno che** non **si tratta** più solo di una serie di adempimenti da gestire ma **di un processo organizzativo aziendale che ha natura produttiva e non solo normativa**.

Il futuro

Nella gestione delle attività di trattamento dei dati si passa dalla **Compliance** all'**Assessment**.

Occorre prepararsi alla **nuova era** del

Privacy Impact Assessment e del **Compliance Risk Management**.

È sempre più evidente che i dati personali sono la nuova materia prima che genera il fatturato delle imprese.

La materia prima va gestita con modelli organizzativi evoluti ed efficienti e comprendendo che si tratta di un tema strategico per le imprese.

Per informazioni aggiornamenti e contatti

Studio Legale Maglio & Partners

Piazza Sant'Agostino, 24

20123 Milano

Tel. 02 43510840

email info@maglio.eu

www.maglio.eu