Il nuovo regolamento europeo in materia di dati personali.

Dieci cose da sapere e dieci cose da fare per gestire al meglio le regole attuali e prepararsi alle nuove norme

a cura dell'Avvocato Marco Maglio

La civiltà dell'informazione ha generato la tutela dei dati personali

La *data protection* è il diritto ad esercitare un controllo sulle informazioni che ci riguardano, evitando che vengano trattate abusandone, per ledere i diritti individuali

- E' un diritto di massa (riguarda tutti)
- E' un diritto dinamico (segue i dati)
- E' un diritto che permette all'individuo di sviluppare la sua personalità in relazione con la collettività (permette l'espansione sociale ed economica).
- Non si identifica con la privacy ma è la sua evoluzione
- Oggi i dati personali sono l'essenza stessa della nostra identità
- Sono generati da ogni nostra azione basata su strumenti informatici
- Possono essere copiati e riutilizzati a basso costo e con strumenti semplici da utilizzare
- Sono diventati la merce di scambio nella società tecnologica: Dati personali in cambio di servizi

Le due domande essenziali

A cosa servono i dati personali?

1) A creare prodotti innovativi
2) A formulare offerte mirate ai consumatori, trasformando gli sconosciuti in clienti fidelizzati
3) A garantire sicurezza e migliorare l'efficienza
4) A controllare e discriminare
5) A profilare e analizzare

Quanto valgono i dati personali?

1) Tanto perché oggi proteggere i propri dati personali significa spesso rinunciare a prodotti e servizi
2) Tanto perché i dati personali sono la materia prima della società dell'informazione
3) Dipende da ciò cui si è disposti a rinunciare per ottenerla: la protezione dei dati è sempre più frutto di un analisi di costo-beneficio.

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.

2) 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.

3) Nel 2012 la Commissione Europea ha deciso di adottare un Regolamento europeo per abrogare la direttiva 95/46 in materia di protezione dei dati personali e, per quanto riguarda il nostro ordinamento, anche le relative disposizioni contenute nel Codice in materia di protezione dei dati personali. Non tutte le norme del Codice saranno però abrogate, rimanendo inalterate quelle di attuazione della Direttiva 2002/58 e quelle della Direttiva 2009/136.

Il Regolamento Generale sulla protezione dei dati

Avremo un testo unico, senza necessità di leggi di recepimento nazionali, valido in tutti i 28 paesi membri dell'Unione Europea.

Non saranno necessarie leggi nazionali di recepimento come avviene per le direttive.

Il 14 aprile 2016 è stato approvato dal Parlamento Europeo il testo definitivo del regolamento che ora attende la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea.

Si spinge fortemente per la minimizzazione del trattamento dei dati.

I nuovi imperativi sono:

1) Tratta meno dati che puoi

2) Favorisci l'anonimizzazione e la pseudonimizzazione.

Ci saranno cambiamenti terminologici rilevanti: nel linguaggio europeo non si userà più l'espressione Titolare del trattamento.

L’impatto del regolamento sulle imprese

Il Regolamento pur con molte mediazioni stabilisce nuovi diritti sul trattamento dei dati personali:
•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.

La gestione dei dati personali non sarà più solo un **adempimento**
È diventata un processo aziendale che incide sull’organizzazione delle imprese.

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

Vediamo quali sono **le dieci cose da sapere su questa riforma e che impatto determina la nuova normativa sulla vita delle imprese.**.

1) A chi si applica la normativa

Le norme interesseranno tutti quei soggetti (anche extraeuropei) che sono chiamati a trattare (in maniera automatizzata o meno) i dati relativi, per esempio, a clienti, dipendenti, studenti, utenti, fornitori.

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.

E' 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.

2) 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

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, indicando obbligatoriamente - per ognuno di essi - una serie "nutrita" 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).
Tutte le operazioni di trattamento devono essere tracciabili e documentabili.
E' la logica della «scatola nera».

3) Cambia l' informativa da rendere all'interessato

Va resa

- in forma concisa,
- trasparente,
- intelligibile e
- facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Le informazioni sono fornite per iscritto o con altri mezzi, se del caso in formato elettronico.

Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Andrà precisato il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare questo periodo-

Se i dati non sono stati raccolti presso l'interessato andrà indicata l'origine del dato

4) Cambia il consenso

Sono quattro le caratteristiche essenziali del consenso per l'uso dei dati a fini commerciali: infatti è valida qualsiasi manifestazione di volontà

1) Libera,
2) Specifica
3) **Informata**
4) Inequivocabile

con la quale l'interessato accetta, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Non è più richiesto il requisito del consenso espresso se non per le attività di profilazione.

Si aprono spazi maggiori per la raccolta di un consenso manifestato attraverso i comportamenti positivi dell'interessato.

Sono in ogni caso illegittimi i consensi raccolti con caselle prebarrate.

5) 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.

Il PIA andrà realizzata per trattamenti potenzialmente rischiosi

Occorrerà:

1. Condurre l'analisi dei rischi

1. Definire i Gap rispetto alla corretta gestione dei rischi

1. Stabilire un Action Plan per colmare questi Gap

1. Controllare annualmente gli interventi effettuati per ridurre i rischi

6) Abolizione della Notificazione

Viene abolito l'obbligo di Notificazione di specifici trattamenti all'Autorità Garante.

Tale adempimento è considerato dal Legislatore europeo come un obbligo che comporta oneri amministrativi e finanziari senza aver mai veramente contribuito a migliorare la protezione dei dati personali (in particolare per le piccole e medie imprese).

È pertanto necessario (continua il testo del Regolamento) abolire tale obbligo generale di notificazione e sostituirlo con meccanismi e procedure efficaci che si concentrino piuttosto su quelle operazioni di trattamento che potenzialmente presentano rischi specifici per i diritti e le libertà degli interessati, per la loro natura, portata o finalità.

Tali trattamenti richiederanno l'effettuazione della valutazione di impatto nel trattamento dei dati.

7) 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.

Le categorie che dovranno nominarlo sono
A)Tutte le autorità ed organismi pubblici

A)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. persone (c.d. interessati) o tipologie di dati che per natura, oggetto o finalità siano definite categorie "a rischio" dalla normativa.

A)Il DPO deve essere designato come soggetto referente del Garante e opera con ampia autonomia e competenza professionale. Può essere un soggetto esterno e il suo mandato, revocabile e rinnovabile, dura quattro anni.

7) I compiti del DPO

1. **sensibilizzare e consigliare** il Titolare in merito agli obblighi (misure e procedure tecniche e organizzative) derivanti dal Regolamento;
2. **sorvegliare** sull'applicazione delle regole di trattamento compresa l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e l'effettuazione degli audit connessi;
3. **sorvegliare** sull'applicazione del Regolamento, con particolare riguardo alla protezione fin dalla progettazione, alla protezione di default, alla sicurezza dei dati, alle informazioni dell'interessato ed alle richieste degli stessi per esercitare i diritti riconosciuti;
4. **controllare** che il Titolare effettui la Valutazione d'impatto sulla protezione dei dati (c.d. DPIA) e richieda all'Autorità di Controllo l'autorizzazione preventiva o la consultazione preventiva nei casi previsti;
5. **fungere** da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento e consultarla, se del caso, di propria iniziativa;
6. **informare** i rappresentanti del personale (es. rappresentanti sindacali) sui trattamenti che riguardano i dipendenti.

8) 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.

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.

9) Obblighi di segnalazione in caso di Violazione sui dati

Con la nozione di violazione dei dati personali (c.d. "**personal data breaches**"), si intende: la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati.

I Titolari del trattamento, in caso di una violazione come sopra descritta, 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).
- Il mancato rispetto di questo obbligo comporta sanzioni penali

10) Riconoscimento di nuovi diritti

Il testo del Regolamento riconosce nuovi diritti agli interessati.

In particolare si fa riferimento a

- **Diritto all'oblio** (right to be forgotten / right to erasure)
- **Diritto alla portabilità del dato** (data portability)

Con Diritto alla portabilità del dato si intende il riconoscimento sia del diritto dell'interessato a **trasferire** i propri dati (es. quelli relativi al proprio "profilo utente") da un sistema di trattamento elettronico (es. Social Network) ad un altro senza che il Titolare possa impedirlo, sia del diritto di **ottenere gli stessi in un formato elettronico strutturato e di uso comune** che consenta di farne ulteriore uso.

Tale diritto deve sempre trovare applicazione quando l'interessato ha fornito i dati al sistema di trattamento automatizzato acconsentendo al trattamento o in esecuzione di un contratto.

C’è un undicesima cosa da sapere:

l' undicesima cosa da sapere sulla riforma

11) La riforma crea nuove opportunità per le imprese

a) **Nuovo valore per i dati personali**: la riforma spinge le imprese ad organizzare bene i dati di cui dispongono valorizzandoli e aggiornandoli. I database sono un asset da valorizzare nel bilancio aziendale

b) **Consenso non equivoco**: la riforma dà spazio a forme di consenso desunto da comportamenti concludenti attivi. Il consenso non deve più essere necessariamente esplicito. Si passa dall'opt in a forme di consenso desumibile per il fatto che la persona ha ricevuto l'informativa e non si è opposta al trattamento dei suoi dati eseguendo un'azione positiva con la quale ha scelto di consentire l'uso dei dati.

c) **Si chiarisce cos’è la profilazione**: la riforma chiarisce che la profilazione consiste nell'analisi di dati cui fa seguito un'azione automatica senza l'intervento dell'uomo. Se si analizzano con strumenti informatici i dati presenti nei propri archivi e poi l'elaborazione dei dati stessi viene sottoposta alla valutazione di una persona prima dell'utilizzo dei dati stessi, per adattare e verificare i dati stessi, non si effettua profilazione. Non occorre un consenso specifico per svolgere tale attività di analisi.

Le sanzioni

Diventano molto più pesanti:

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.

Tempi di recepimento

Il regolamento approvato il 14 aprile 2016 entrerà in vigore in via definitiva due anni dopo la sua pubblicazione in Gazzetta Ufficiale dell'Unione Europea.

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.

Per l'Italia bisognerà affrontare queste essenziali novità:

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

Le 10 cose da fare ora

1) Informare le persone all'interno della vostra organizzazione dei cambiamenti in arrivo per valutare i possibili impatti.

2) Analizzare quali sono i dati di cui si dispone e fare una mappatura aggiornata dei dati

3) 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. Sperimentare nuove forme di informative visulai basate su icone.

4) Definire ora le regole di gestione dei diritti dell'interessato e valutare cosa significa gestire il diritto all'oblio

5) Analizzare i processi di gestione delle istanze degli interessati e verificare come gestire questi processi avvalendosi di sistemi informatici e user friendly

6) Analizzare gli effetti del diritto alla portabilità dei dati e adottare cautele organizzative per evitare impatti gravi sulla stabilità dei data base aziendali

Le 10 cose da fare ora

7) Definire le nuove regole di acquisizione e documentazione del consenso. Verificare con cura i fornitori dei dati. Questo è il tempo in cui fare test, test e ancora test. Verificare se trattate dati di minori e tenere conto che le nuove regole impongono di gestire anche il consenso degli esercenti la potestà dei genitori insieme al consenso del minore al di sotto dei 16 anni.

8) Dotarsi di “software sentinella” per gestire il nuovo obbligo di notifica delle violazioni nell’uso dei dati personali.Verificare l’eventuale flusso extraeuropeo dei dati usando servizi cloud.

9) Sperimentare la Privacy by Design e effettuare tempestivamente 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.

10) Pensare a come gestire la funzione di Responsabile per la protezione dei dati personali all’interno dell’azienda. Sarà un cambiamento organizzativo essenziale e va impostato ora.

E non finisce qui….

50 dei 99 articoli del Regolamento Europeo rimandano a norme attuative e norme nazionali di esecuzione.

Anche i Garanti nazionali emaneranno norme per anticipare l'entrata in vigore di alcuni aspetti del Regolamento e favorire l'armonizzazione tra i diversi ordinamenti.

Quindi nei prossimi mesi ci sarà molto da fare per adeguarsi alle nuove norme.

Per le aziende che trattano in modo significativo dati personali sarà importante definire un action plan e attivare un processo di adeguamento che segua costantemente le novità che si susseguiranno.

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 teleselling e più in generale di trattamento dei dati si passa

dalla **Compliance**

all'**Assessment**

Occorre prepararsi alla nuova era del Privacy Impact Assessment e del Compliance Risk Management.

E' 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.

GRAZIE PER L'ATTENZIONE

Per informazioni e aggiornamenti

WWW.MAGLIO.EU

Dal 15 maggio 2016
WWW.OSSERVATORIOPRIVACY.IT

Da GIUGNO SU PROMOTION MAGAZINE

OSSERVATORIO DIRITTO & MARKETING

Per contatti info@maglio.eu