NUOVA PRIVACY ED ADEMPIMENTI PER IMPRESE E PROFESSIONI

DANIELE DONDARINI

SEGRETERIA ANTOI

COSA C'E' DIETRO L'ANGOLO

- *Il 25 gennaio 2012 la Commissione europea ha presentato ufficialmente le proposte relative al nuovo quadro giuridico europeo in materia di protezione dei dati. Si tratta di un Regolamento, che andrà a sostituire la direttiva 95/46/CE, e di una Direttiva che dovrà disciplinare i trattamenti per finalità di giustizia e di polizia (attualmente esclusi dal campo di applicazione della direttiva 95/46/CE).*
- *A dicembre 2015 è stato approvato il testo definitivo.*
- ***Il nuovo Regolamento è stato pubblicato sulla GUUE L 119 del 4 maggio 2016.***

KICK OFF

Articolo 99 Entrata in vigore e applicazione

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale dell'Unione europea

> 24 maggio 2016

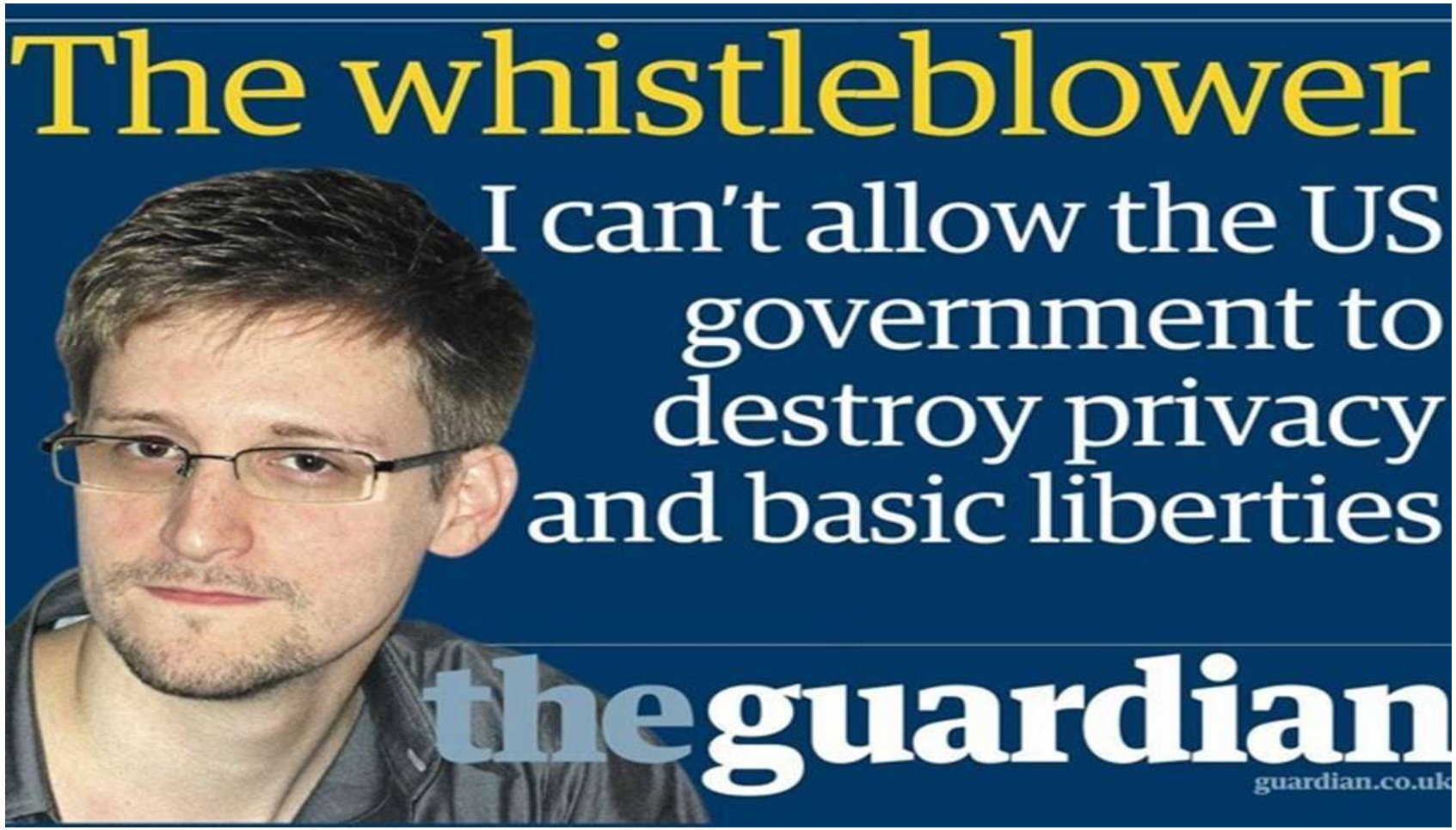
Esso si applica a decorrere dal 25 maggio 2018

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

ARTICOLO 5
PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

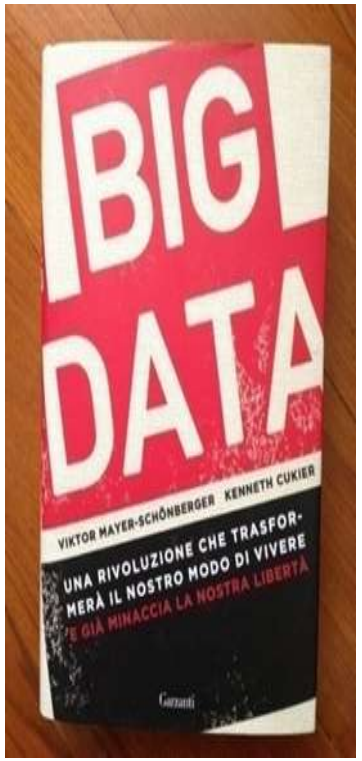
- ***Liceità, correttezza e trasparenza:*** *trattamento lecito, corretto e trasparente*
- ***Limitazione della finalità:*** *raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità*
- ***Minimizzazione dei dati:*** *adeguati, pertinenti e limitati a quanto necessario*
- ***Esattezza:*** *esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti*
- ***Limitazione della conservazione:*** *conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità*
- ***Integrità e riservatezza:*** *trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*

PERCHE' APPROCCI SEMPRE PIU' VINCOLANTI?



ACCOUNTABILITY - *CAPO IV TITOLARE E RESPONSABILE*

- ***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 presente regolamento***
- ***In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.***



GLI ATTORI PRINCIPALI E LE RESPONSABILITA'

- ***Titolare del trattamento:*** *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri,* ***determina le finalità e i mezzi del trattamento di dati personali***
- ***Responsabile del trattamento:*** ***la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (CULPA IN ELIGENDO 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 ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato)***
- ***I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto stipulato in forma scritta, anche in formato elettronico (IL REGOLAMENTO STABILISCE I CONTENUTI MINIMI DEL CONTRATTO)***

Dati acquisiti e poi successivamente utilizzati per finalità completamente differenti da quelle dichiarate

Un passante notò due grossi sacchi di plastica azzurra abbandonati in mezzo alla via. Incuriosito, si avvicinò e si rese conto che in essi si trovavano cartelle cliniche di un ospedale.

Nel corso del trasporto da una sede all'altra, l'autista del furgone non aveva fissato solidamente i sacchi contenenti le cartelle cliniche, per cui nel trasporto due di questi erano caduti a terra, senza che egli se ne accorgesse. Il Garante ha sanzionato sia l'Ospedale sia l'autista, in quanto egli operava sotto la responsabilità dell'ente ospedaliero.

Dati conservati per periodi indefiniti, molto lunghi, spesso "per sempre"

GLI ALTRI PROTAGONISTI OLTRE AGLI INTERESSATI

- **"*Incaricato del trattamento*": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento**
- **Chi è il Responsabile della protezione dei dati o, anche, Data Protection Officer?**

UNA NOVITÀ PER LE AZIENDE ORTOPEDICHE … LA DESIGNAZIONE DI UN DATA PROTECTION OFFICER

Il Regolamento introduce la figura del "Responsabile per la protezione dei dati" o Data Privacy Officer (DPO). Che non è un semplice responsabile del trattamento ma un manager del trattamento dei dati.

Le categorie che dovranno nominarlo sono:

A. **Tutte le autorità ed organismi pubblici**

B. **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, come i dati idonei a rivelare lo stato di salute.**

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

The role of a data protection officer

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);
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.

NUOVI ADEMPIMENTI

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».

LA GESTIONE DEI DATI PERSONALI NON SARÀ PIÙ SOLO UN ADEMPIMENTO È DIVENTATA UN PROCESSO AZIENDALE CHE INCIDE SULL'ORGANIZZAZIONE DELLE IMPRESE.

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:

Condurre l'analisi dei rischi

Definire i Gap rispetto alla corretta gestione dei rischi

Stabilire un Action Plan per colmare questi Gap

Controllare annualmente gli interventi effettuati per ridurre i rischi

PROCESSI PER LA PROTEZIONE DEI DATI

OVVIAMENTE DOVREMO CAMBIARE ANCHE L'INFORMATIVA, QUANDO AVREMO NOMINATO IL DPO!

- 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.

IDENTICAMENTE, SI MODIFICA LA PROCEDURA DEL CONSENSO

Sono quattro le caratteristiche essenziali del consenso per l'uso dei dati; infatti è valida qualsiasi manifestazione di volontà purché Libera, Specifica, Informata ed 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.

Per profilazione si intende l'analisi e l'elaborazione di informazioni relative a utenti o clienti, al fine di suddividere gli interessati in "profili", ovvero in gruppi omogenei per comportamenti o caratteristiche; tale categorizzazione è generalmente strumentale sia alla messa a disposizione di servizi sempre più mirati e conformati sulle specifiche esigenze dell'utente sia a conformare messaggi pubblicitari per destinarli a specifici profili di utenti.

SI INTRODUCE UN OBBLIGO DI SEGNALAZIONE IN CASO DI VIOLAZIONE DI 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

NUOVI DIRITTI PER L'INTERESSATO

- **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.

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.

GRAZIE PER L'ATTENZIONE!