

**Privacy e information
security alla luce del
nuovo Regolamento UE**

**Udine, Sala Valduga
14 marzo 2016**

Avv. David D'Agostini

Relatore

Avvocato cassazionista

**Professore a contratto di
Informatica e diritto**

**Fondatore del
Centro Innovazione e Diritto**

Diritto dell'informatica

**Proprietà intellettuale e
industriale**

**E-commerce e concorrenza
on line**

**Reati informatici e digital
forensics**

Sicurezza informatica e privacy

“Privacy”

1890

The right to be let alone

Oggi

**Data protection = diritto al
controllo delle informazioni
personali**

Normativa attuale

Direttiva 1995/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

Legge 31 dicembre 1996 n. 675 (abrogata)
D.lgs. 30 giugno 2003 n. 196

A breve

Proposta di regolamento COM (2012) 11 concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati

Abrogherà la Direttiva 1995/46/CE (non la Direttiva 2002/58/CE)

Applicazione territoriale

1) al trattamento dei dati personali effettuato da **responsabile/incaricato con stabilimento nell'UE**

2) al trattamento dei dati personali relativo all'offerta di beni o alla prestazione di servizi a **interessati nell'UE** ovvero se nell'UE c'è monitoraggio

Definizioni

- Trattamento
- Dato personale
- Consenso dell'interessato (\neq)
- Profilazione (N)
- Pseudonimizzazione (N)
- Violazione di dati personali (N)

Soggetti

Ante

- Interessato
- Titolare
- Responsabile
- Incaricato

=====

Post

- Interessato
 - Responsabile
 - Incaricato
- =====
- Privacy officer

Principi generali

- **liceità, equità e trasparenza**
- **limitazione delle finalità**
- **minimizzazione dei dati**
- **limitazione della conservazione**
- **esattezza**
- **integrità e riservatezza**

Accountability

Responsabilità + rendicontazione

- 1) Garantire che il trattamento dei dati sia conforme al Regolamento
- 2) Essere in grado di dimostrarlo!

Adozione di un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati

Nuovo approccio

Privacy by design

Tutela dei diritti e delle libertà dell'interessato sin dalla “progettazione” (integrazione nel ciclo tecnologico)

Privacy by default

Le impostazioni predefinite devono essere quelle che garantiscono il massimo livello di privacy

Informativa

Per **iscritto** (oralmente su richiesta dell'interessato, purché ne sia comprovata con altri mezzi l'identità)

Forma concisa, trasparente, intelligibile e facilmente accessibile, con linguaggio semplice e chiaro

Consenso

Caratteristiche del consenso:

- espresso (azione positiva inequivoca)
- informato, libero e specifico
- revocabile

Consenso esplicito in caso di categorie particolari di dati e di profilazione

Casi di esclusione del consenso

Notifica

Viene abolito l'obbligo di
notificazione al Garante nel caso
di specifici trattamenti

(risparmio di € 130 milioni all'anno)

Valutazione d'impatto

Privacy Impact Assessment

Prima di procedere a un trattamento che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (in considerazione della natura, del campo di applicazione, del contesto e delle finalità del trattamento stesso)

Privacy Officer

Dev'essere designato in caso di:

- trattamento effettuato da un'autorità o un organismo pubblico
- controllo regolare e sistematico degli interessati su larga scala
- trattamento, su larga scala, di “dati sensibili”

Compiti del Privacy Officer

- informare e consigliare il Responsabile
- sorvegliare l'osservanza del Regolamento
- dare il parere sulla Valutazione d'impatto
- cooperare con l'Autorità di controllo
- fungere da punto di contatto

Viene prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali

Diritti dell'interessato

- **diritto di accesso** (origine dei dati; finalità e modalità del trattamento; categorie di dati; periodo di conservazione; diritto di proporre reclamo)
- **diritto di rettifica** (dati inesatti)
- **diritto di integrazione** (dati incompleti)

Diritto all'oblio

Cancellazione dei dati personali nei casi in cui:

- non sono più necessari rispetto alle finalità
- l'interessato revoca il consenso
- l'interessato si oppone al trattamento
- sono stati trattati illecitamente
- sussiste un obbligo legale

Right to be forgotten

Corte di Giustizia UE - Decisione 13 maggio 2014

Eliminare dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, i link verso pagine web pubblicate da terzi e contenenti informazioni relative a tale persona (cd. deindicizzazione)

Oblio vs. Cronaca

Diritto all'oblio bilanciato con diritto di cronaca, libertà d'espressione e di informazione

Linee Guida Data Protection Working Party del 26 novembre 2014

Tribunale Roma, sentenza del 3 dicembre 2015

Finalità giornalistiche

- **Verità** (anche solo putativa)
- **Continenza** della forma espositiva
- **Pertinenza** o interesse alla notizia

Art. 137 d.lgs. 196/03 e codice deontologico stabiliscono il principio di **essenzialità** dell'informazione

- **Esenzioni/deroghe** nel Reg. UE

Sicurezza

Responsabile/Incaricato attuano misure tecniche e organizzative adeguate per garantire un **livello di sicurezza adeguato** al rischio

- pseudonimizzazione e cifratura
- riservatezza, disponibilità, integrità
- disaster recovery
- procedura di audit

Data Breach

Il Responsabile **notifica** senza ritardo la violazione all'Autorità di controllo:

- describe la natura della violazione
- **indica il Privacy Officer**
- describe le probabili conseguenze
- **indica le misure adottate per rimediare**

Violazione è **comunicata** all'interessato se c'è elevato rischio per suoi diritti

Danni

Il Responsabile/l'Incaricato che cagiona danno trattando dati personali è tenuto al risarcimento, salvo dimostri che l'evento non gli è imputabile

Ogni Responsabile/Incaricato risponde per l'intero danno

Sanzioni

Sanzioni efficaci, proporzionate e dissuasive tenuto conto di:

- natura, gravità e durata della violazione
- **violazione dolosa o colposa**
- misure per attenuare il danno
- **grado di responsabilità**
- precedenti violazioni
- **cooperazione con l'Autorità**

Prof. Avv. David D'Agostini

www.avvocatidagostini.it

studio@avvocatidagostini.it

Via Vittorio Veneto 32 - Udine

Centro Innovazione & Diritto



www.cindi.it
info@cindi.it

