*Corso di alta formazione sulla Protezione dei Dati Personali per Responsabile della protezione dei dati (DPO)*
**II EDIZIONE 2018**

## Disciplina generale – Dal Codice Privacy al RGPD

# Introduzione

Avv. Giuseppe Busia

**Consiglio Nazionale Forense – Consiglio Nazionale Ingegneri**

**19 maggio 2018**

# Dove sono i dati personali

- La civiltà della sorveglianza
  - Telecamere intelligenti, rilevazioni biometriche, *RFID*, sistemi di localizzazione, IOT, ecc.
- Noi siamo le tracce che lasciamo
  - Crescono quanto più i servizi sono sofisticati
  - Cloud evoluto
- L'identità costruita sulla base di esse
  - Intelligenza artificiale e Machine learning

# Lo sviluppo delle banche dati

- Sviluppo tecnologico e conservazione dei dati
  - Aumenta la capacità di memoria
  - Si accrescono i tempi di conservazione
  - Si moltiplicano le interconnessioni fra banche dati
  - Diventa meno costoso conservare i dati
    - Un esempio: i motori di ricerca

# Memoria e oblio

- Diritto all'oblio come diritto di libertà
  - Di scegliere liberamente
  - Di cambiare e di correggersi (Identità)
- I nemici dell'oblio
  - Le capacità tecniche di conservazione dei dati
  - La nostra pigrizia
- La sentenza Google Spain
- Il nuovo Regolamento
- Oblio e sicurezza
  - Dalla contrapposizione alla complementarietà

# Perché valgono tanto

- Rischi di sottovalutazione
  - Non è un gioco da ragazzi
  - Non è virtuale
- Il valore dei dati
  - Economico
    - Dopo l'oro giallo e l'oro nero…la profilazione
  - Strategico
    - La nuvola europea
    - Verso un Privacy Schield
  - Sicurezza: criminalità comune e organizzata
  - Politica: dalla consultazione permanente alla profilazione degli elettori

# Una diversa normativa sulla trasparenza della PA

- Uno strumento di trasparenza e di controllo sull'agire amministrativo
  - Se la PA deve dire che uso fa delle informazioni dei cittadini, deve anche mostrare come lavora
- La mappatura normativa di ogni azione
  - Più dettagliata per le informazioni più delicate
  - Il principio di finalità
- Autorizzazione normativa, informativa, diritto d'accesso…
- Le misure di sicurezza contro gli usi impropri

*Corso di alta formazione sulla Protezione dei Dati Personali per Responsabile della protezione dei dati (DPO)*
**II EDIZIONE 2018**

## Disciplina generale

# Dal Codice Privacy al Regolamento generale UE

Avv. Giuseppe Busia

**Consiglio Nazionale Forense – Consiglio Nazionale Ingegneri**

**19 maggio 2018**

# Una normativa in continua evoluzione

- Le leggi 31 dicembre 1996, nn. 675 e 676 e le successive deleghe
  - Dal diritto ad essere lasciati soli al controllo sui propri dati
- I decreti delegati fino al d.lgs. 467/2001
- Gli atti paranormativi e le pronunce del Garante
- **Il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196)**

# La mappa del Codice privacy

- **Parte I: Disposizioni generali**
- **Parte II: Disposizioni relative a specifici settori**
  - Trattamenti in ambito giudiziario (artt. 46 ss.)
  - Trattamento da parte di forze di polizia (artt. 53 ss)
- **Parte III: Tutela dell'interessato e sanzioni**
- Allegati
  - A) I Codici deontologici
  - B) Disciplinare tecnico in materia di misure minime di sicurezza
  - C) Trattamenti in ambito giudiziario e per fini di polizia (vedi slides seguenti)

# I Codici di deontologia (1)

**Differenze con i Codici di Condotta (art 40 RGPD – rinvio)**

- Codici di deontologia e di buona condotta per determinati settori
- Il Garante promuove la sottoscrizione
  - Nell'ambito delle categorie interessate
  - Nell'osservanza del principio di rappresentatività
  - Tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa
- Verifica la conformità alle leggi ed ai regolamenti, anche attraverso l'esame di osservazioni di soggetti interessati

# I Codici di deontologia (2)

- **Il rispetto di *tutti* è condizione essenziale per la liceità dei trattamenti**
  - **Anche il codice dei giornalisti**
- Pubblicati sulla Gazzetta Ufficiale
- Riportati in allegato al Codice privacy (allegato A)
  - Con decreto del Ministro della giustizia
- Il Garante contribuisce a garantirne la diffusione ed il rispetto

# Le regole deontologiche (1)

Il Garante promuove, nell'osservanza del principio di rappresentatività e tenendo conto delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, l'adozione di regole deontologiche per i trattamenti previsti dalle disposizioni **di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, e al Capo IX del Regolamento** e ne verifica la conformità alle disposizioni vigenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

# Le regole deontologiche (2)

- Lo schema di regole deontologiche è sottoposto a consultazione pubblica per almeno sessanta giorni.
- Le regole deontologiche sono pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente decreto.
- Il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali.

# Disposizione transitorie A5 A7

- Allegati A5 e A7 continuano a produrre effetti, sino alla definizione della procedura di cui alla lettera b), a condizione che si verifichino congiuntamente le seguenti condizioni:
- a) entro sei mesi le categorie interessate sottopongano all'approvazione del Garante, a norma dell'articolo 40 del Regolamento, i codici di condotta
- b) la procedura di cui alla lettera a) si concluda entro sei mesi dall'attivazione.
- 2. Le disposizioni contenute nei codici riportati negli allegati A1, A2, A3, A4 e A6 del Codice in

# Disposizione transitorie

- Allegati **A1, A2, A3, A4 e A6** sono **ridenominate regole deontologiche** e continuano a produrre effetti, in quanto compatibili con le disposizioni del Regolamento, e sono pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono successivamente riportate nell'allegato A) del presente decreto.
- Il Garante ne promuove la revisione sulla base delle disposizioni sulle regole di condotta

# Disposizione transitorie A5 A7

- Allegati **A5 e A7** continuano a produrre effetti, sino alla definizione della procedura di cui alla lettera b), a condizione che si verifichino congiuntamente le seguenti condizioni:
- a) entro sei mesi le categorie interessate sottopongano all'approvazione del Garante, a norma dell'articolo 40 del Regolamento, i **codici di condotta**
- b) la procedura di cui alla lettera a) si concluda entro sei mesi dall'attivazione

# I pilastri della tutela
## (Codice Privacy)

- Informativa
- Consenso
  - Autorizzazione
    - Base normativa per soggetti pubblici (v. seguente)
- Diritti dell'interessato
- Misure di sicurezza
- Notificazione
  - Differenze col Regolamento Generale (rinvio)

*Corso di alta formazione sulla Protezione dei Dati Personali per Responsabile della protezione dei dati (DPO)*
**II EDIZIONE 2018**

**Disciplina generale – Dal Codice Privacy al RGPD**

# Le principali novità del RGPD

Avv. Giuseppe Busia

**Consiglio Nazionale Forense – Consiglio Nazionale Ingegneri**

**19 maggio 2018**

# Il Regolamento UE n. 679 del 2016

- **Il «pacchetto» con la direttiva ex Terzo pilastro**
  - Proposta della Commissione
  - L'iter di approvazione fra Parlamento e Consiglio
  - Il Gruppo ex art. 29 della Direttiva 95/46
  - La conclusione del Trilogo nel dicembre 2015
- **Una legge unica europea**
- **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

# Stabilimento principale (a)

- a) titolare con **stabilimenti in più di uno Stato membro**, il luogo della sua amministrazione centrale nell'Unione,
- **salvo che** le **decisioni sulle finalità e i mezzi** del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni
  - In quest'ultimo caso lo stabilimento che ha adottato tali decisioni è considerato stabilimento principale

# Stabilimento principale (b)

- b) **responsabile** del trattamento con **stabilimenti in più di uno Stato membro**, il luogo in cui ha sede la sua amministrazione centrale nell'Unione
- **o,** se il responsabile non ha un'amministrazione centrale nell'Unione, lo stabilimento nell'Unione in cui sono condotte le **principali attività di trattamento** nel contesto delle attività di uno stabilimento del responsabile del trattamento
  - nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento

# Ambito di applicazione (1)

- Trattamenti effettuati nell'ambito di uno stabilimento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione
  - Effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile
- Si applica anche al trattamento effettuato da un titolare che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico

# Ambito di applicazione (2)

- Trattamenti riguardanti interessati che si trovano nell'Unione, effettuato da un **titolare o da un responsabile che non è stabilito nell'Unione**, quando le attività di trattamento riguardano:
- a) l'offerta di **beni o servizi a interessati nell'Unione**, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
- b) il **monitoraggio** del loro comportamento se tale comportamento ha luogo all'interno dell'Unione

# Quadro generale del RGPD (1)

- **Responsabilizzazione del titolare**
  - **Ciascuno si conosce meglio di quanto possa farlo l'Autorità**
- **Valutazione di impatto sulla protezione dei dati**
  - **Fin dalla progettazione del trattamento**
    - **Privacy by design**
    - **Privacy by default**
- **Misure di sicurezza basate sul rischio**
  - **Approccio basato sul rischio**
  - **Consultazione preventiva dell'Autorità**

# Quadro generale del RGPD (2)

- **Codici di condotta (associativi)**
- **Responsabile della protezione dati (artt. 37 ss. - rinvio)**
- **Estensione obbligo di notifica all'Autorità delle violazioni dei dati personali (art. 33)**
  - **Senza ingiustificato ritardo e, ove possibile , entro 72 ore**
  - **Possibile comunicazione all'interessato**

# Quadro generale del RGPD (3)

- **Certificazione**
  - **La ripartizione dei ruoli ed i compiti dell'Autorità**
- **Sportello unico al quale rivolgersi**
  - **Possibili criticità per gli interessati**
  - **Individuazione dell'Autorità capofila in base allo stabilimento principale e altri criteri**
- **Sanzioni**
- **Diritti rafforzati**
  - **Portabilità, Oblio (rinvio)**

*Corso di alta formazione sulla Protezione dei Dati Personali per Responsabile della protezione dei dati (DPO)*
**II EDIZIONE 2018**

## Disciplina generale – Dal Codice Privacy al RGPD

# Principi generali a confronto

Avv. Giuseppe Busia

**Consiglio Nazionale Forense – Consiglio Nazionale Ingegneri**

**19 maggio 2018**

# Alcuni principi generalissimi
## (Art 11 Codice – Cfr Art. 5 RGPD)

I dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

# Principi applicabili ex Art. 5 (1)

I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

- un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

(segue)

# Principi applicabili ex Art. 5 (2)

d) esatti e, se necessario, aggiornati;

- devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»)

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

- i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione») (segue)

# Principi applicabili ex Art. 5 (3)

f) trattati in maniera 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 («integrità e riservatezza»)

- **Il titolare del trattamento**
  - **È competente per il rispetto dei principi (paragrafo 1)**
  - **È in grado di comprovarlo**
    - **(«responsabilizzazione»).**

*Corso di alta formazione sulla Protezione dei Dati Personali per Responsabile della protezione dei dati (DPO)*

**II EDIZIONE 2018**

## Disciplina generale – Dal Codice Privacy al RGPD

# Dati personali e loro tipologie

Avv. Giuseppe Busia

**Consiglio Nazionale Forense – Consiglio Nazionale Ingegneri**

**19 maggio 2018**

# I dati personali nella normativa italiana

- Qualunque informazione relativa a:
  - **persona fisica**
  - *[persona giuridica, ente od associazione]*
    - *DL n. 201/2011, (convertito in legge n. 214/2011)*
- Identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale

# I dati personali nel RGPD

- Qualsiasi informazione
- Riguardante una **persona fisica**
- Identificata o identificabile («interessato»)

- **La figura dell'interessato**

- Idendificabilità (rinvio)

# Quando una persona è identificabile?

- Quando la persona fisica può essere identificata, direttamente o indirettamente
  - con particolare riferimento a un identificativo come il nome, un numero di identificazione,
  - dati relativi all'ubicazione, un identificativo online
  - o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

# La Pseudonimizzazione

- il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico **senza l'utilizzo di informazioni aggiuntive,**
  - **a condizione** che tali informazioni aggiuntive:
    - siano conservate separatamente
    - e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile

# I dati sensibili nel Codice privacy

- Il “nocciolo duro” della riservatezza
- Quelli idonei a rivelare (art.4, comma 1,lett.d):
  - l’origine razziale ed etnica,
  - le convinzioni religiose, filosofiche o di altro genere nonché le opinioni politiche,
  - l’adesione **a partiti,** sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, o sindacale,
  - lo stato di salute o la vita sessuale
- Evitare le interpretazioni troppo estensive

# Categorie particolari di dati personali (art. 9)

1. È vietato trattare dati personali che rivelino:
   - l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati **genetici**, dati **biometrici** intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

(Rinvio sul regime applicabile)

# I dati relativi alla salute nel GDPR

- I dati personali
- attinenti alla salute fisica o mentale
- di una persona fisica
  - compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute

# I dati biometrici nel GDPR

- I dati personali ottenuti da un trattamento tecnico specifico relativi alle **caratteristiche**
  - **fisiche,**
  - **fisiologiche**
  - **o comportamentali**
- che consentono o confermano l'**identificazione univoca** di una persona fisica
  - quali l'immagine facciale o i dati dattiloscopici

# I dati genetici nel GDPR

- I dati personali relativi alle caratteristiche genetiche
- ereditarie o acquisite di una persona fisica
- che forniscono informazioni univoche
- sulla fisiologia o sulla salute di detta persona fisica,
- e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione

# I dati giudiziari nel Codice privacy

- I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la **qualità di imputato o di indagato** ai sensi degli articoli 60 e 61 del codice di procedura penale
  - Art.4, comma 1,lett.e)

# Art. 10- Trattamento dei dati personali relativi a condanne penali e reati (1)

- Il trattamento dei dati personali relativi
  - alle condanne penali e ai reati o a connesse misure di sicurezza
- sulla base dell'articolo 6, paragrafo 1 (consenso, contratto, obbligo legale, interessi vitali…)
- deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri **o** se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri
  - che preveda garanzie appropriate per i diritti e le libertà degli interessati.

# Art. 10- Trattamento dei dati personali relativi a condanne penali e reati (2)

- Un eventuale **registro completo delle condanne penali**
  - deve essere tenuto soltanto sotto il controllo dell'autorità pubblica

# Grazie dell’attenzione!