La normativa Europea sulla privacy

Fondamenti Normativi

Regolamento 679 del Parlamento Europeo 27/04/2016

173 Considerando

99 articoli

La normativa Europea sulla privacy

Principi Fondamentali

Privacy: the right of an individual to be let alone

Fisica: spazio fisico / solitudine

Informativa: gestire le informazioni su sè stessi e decidere cosa e come comunicarle ad altri

(Information Commissioner’s Office [UK] Conductin Privacy Impact Assessments, pg.6)

La normativa Europea sulla privacy

Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali

Art.1 comma 2

La normativa Europea sulla privacy

Definizioni:

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile
Non riguarda i dati anonimi
Non riguarda le persone decedute
Riguarda anche I dati anonimi ma riconducibili a persone fisiche

La normativa Europea sulla privacy

Definizioni:

Trattamento: qualsiasi operazione applicata a dati personali

La normativa Europea sulla privacy

Definizioni:

Limitazione di trattamento: contrassegno di dati personali con l’obiettivo di limitarne il trattamento

La normativa Europea sulla privacy

Definizioni:

Profilazione: trattamento dei dati che consente di prevedere il comportamento futuro

La normativa Europea sulla privacy

Definizioni:

Pseudonimizzazione = +/- anonimizzazione
(ma con l’uso di dati detenuti altrove si può risalire all’interessato)

La normativa Europea sulla privacy

Definizioni:

Titolare: chi determina la finalità e I mezzi del trattamento (quindi può anche non detenere fisicamente I dati?)
Responsabile del trattamento: chi tratta I dati per conto del titolare
Responsabile della protezione dei dati: chi controlla che il trattamento dei dati sia conforme al regolamento (sezione 4)

La normativa Europea sulla privacy

Definizioni:

Destinatario: chi riceve comunicazione dei dati personali

La normativa Europea sulla privacy

Definizioni:

Consenso dell'interessato: qualsiasi manifestazione di volontà … che I dati personali … siano oggetto di trattamento

(può anche non essere scritto ma se è scritto deve rispondere a determinate regole)

La normativa Europea sulla privacy

Definizioni:

Violazione di dati personali:

distruzione
perdita
modifica
divulgazione

accidentale o illecita

La normativa Europea sulla privacy

Principi:

Il trattamento dei dati deve essere

Lecito
Corretto
Trasparente

Art.5

La normativa Europea sulla privacy

Il trattamento è lecito se:

a) l'interessato ha espresso il consenso

b) è necessario per l'esecuzione di un contratto di cui l'interessato è parte

c) è necessario per adempiere un obbligo legale

Art.6 comma 1

La normativa Europea sulla privacy

Principi:

1 È vietato il trattamento di dati … genetici … biometrici … relativi alla salute … alla vita sessuale

Art.9

La normativa Europea sulla privacy

A meno che

2a) l'interessato abbia dato il suo consenso

2h) sia necessario per attività di … diagnosi, assistenza o terapia sanitaria … conformemente al contratto con un professionista della sanità

3) se sono trattati da (sotto la responsabilitò di) un professionista soggetto al segreto sanitario

La normativa Europea sulla privacy

Informazioni raccolte presso l’interessato

Diritti dell’interessato: informativa

Identità del titolare
Finalità e base giuridica del trattamento
Destinatari dei dati

Art.13 comma 1

La normativa Europea sulla privacy

Diritti dell’interessato: informativa

Il periodo di conservazione
Il diritto all’accesso, alla rettifica, alla cancellazione, alla revoca del consenso, a proporre reclamo
Se l’interessato ha l’obbligo di fornire I dati e cosa succede se non li fornisce
Se il titolare intende trattare ulteriormente I dati (per ricerca)

Art.13 comma 2

La normativa Europea sulla privacy

Diritti dell’interessato: di accesso

Diritto di ottenere conferma che sia in corso un trattamento
(finalità, dati trattati, destinatari, periodo di conservazione, rettifica, cancellazione, limitazione, opposizione, diritto di proporre un reclamo)

Art.15 comma 1

La normativa Europea sulla privacy

Diritti dell’interessato: di accesso

Il titolare fornisce
una
copia
dei dati personali oggetto di trattamento

In formato elettronico di uso comune

Art.15 comma 2

La normativa Europea sulla privacy

Diritti dell’interessato: alla portabilità

Formato strutturato di uso comune

Ad un altro titolare

Art.20

La normativa Europea sulla privacy

Diritti dell’interessato

Diritto di rettifica: art.16 (si)

Diritto di cancellazione: art.17 (no)

Diritto di limitazione del trattamento (se ne contesta l’esattezza, è illecito, si è opposto) art.18 (?)

Diritto di opposizione: art.21 (no)

La normativa Europea sulla privacy

Obblighi del titolare

Misure tecniche ed organizzative per garantire che il trattamento è conforme al regolamento

art.24

La normativa Europea sulla privacy

Privacy by design: la raccolta dei dati consente di garantirne la sicurezza sin dalla progettazione

Privacy by default: i dati vengono protetti normalmente e non solo quando ce ne sono ragioni specifiche

art.25

La normativa Europea sulla privacy

Obblighi del titolare

Pseudonimizzazione

I dati non sono accessibili ad un numero indefinito di persone senza l’intervento della persona fisica

art.25

La normativa Europea sulla privacy

Obblighi del titolare

I contitolari hanno I medesimi obblighi

art.26

La normativa Europea sulla privacy

Responsabile del trattamento

Deve essere nominato? No
Se è nominato:
Contratto scritto
Garanzie sufficienti
Nomina altri sub-responsabili con contratto scritto
Ha gli stessi doveri del titolare

Art.28

Deve essere istruito/formato

art.29

La normativa Europea sulla privacy

Obblighi del titolare

Sicurezza del trattamento

Pseudonimizzazione dei dati

Riservatezza (PW)

Integrità, disponibilità, resilienza (Backup)

Valutazione dei rischi di distruzione, perdita, modifica, divulgazione, accesso (PIA art.35)

Formazione degli incaricati del trattamento

Art.32

La normativa Europea sulla privacy

Obblighi del titolare

Notifica di una violazione

all’autorità di controllo: art.33

all’interessato: art.34

La normativa Europea sulla privacy

PIA: Privacy Impact Assesment (art.35)
= DPS

Se c’è un rischio elevato per I diritti e le libertà delle persone fisiche (comma 1)

Se si tratta di un trattamento su larga scala di dati art.9 comma 1 = dati relativi alla salute (comma 3b)

La normativa Europea sulla privacy

PIA

Deve valutare la probabilità e la gravità del rischio
Tenuto conto della natura, del contesto, delle finalità, delle fonti di rischio

Considerando 90

La normativa Europea sulla privacy

PIA

Non è obbligatorio nel caso di dati personali … da parte di un singolo medico, operatore sanitario

Considerando 91

La normativa Europea sulla privacy

PIA: art.35

Raccoglie le opinioni degli interessati

Comma 9

La normativa Europea sulla privacy

PIA

Gravità del rischio:
- dati anagrafici (cellulare?)
- dati di salute → onore? Reputazione?

Probabilità?

La normativa Europea sulla privacy

Registro delle attività di trattamento art.30

Obbligatorio se:

~~Più di 250 dipendenti~~
C’è un rischio per la libertà e i diritti dell’interessato ?
Trattamento stutturato (non occasionale) ?
Dati sanitari ?
~~Dati giudiziari~~

La normativa Europea sulla privacy

Registro delle attività di trattamento: art.30

Dati del titolare del trattamento
Categorie degli interessati e dei dati personali
Categorie dei destinatari
Misure tecniche e organizzative (pseudonimizzazione, pw, backup, chiavi fisiche, ...)

La normativa Europea sulla privacy

Responsabile della protezione dei dati

Obbligatorio? Trattamento su larga scala dei dati di salute art 37 comma 1b

Può essere un dipendente o un professionista comma 6

Non può ricevere istruzioni (direttive) art.38 comma 3

La normativa Europea sulla privacy

Codici di condotta elaborati dalle associazioni

Precisano:
Il trattamento corretto dei dati
La pseudonimizzazione
l'informativa
I diritti degli interessati
…
Art.40 – 41 – 42 (certificazione)

La normativa Europea sulla privacy

Capo V trasferimento dei dati all’estero
Capo VI autorità di controllo
Capo VII cooperazione e coerenza

La normativa Europea sulla privacy

Capo VIII

ricorsi
responsabilità
sanzioni

La normativa Europea sulla privacy

Capo VIII

ricorsi

all’autorità di controllo
Al tribunale ordinario

Art.77-78-79

La normativa Europea sulla privacy

Capo VIII

Danno materiale o immateriale comma 1

Titolare e responsabile in solido comma 2

A meno che non gli sia in alcun modo imputabile comma 3

Art.82

Capo VIII
Sanzioni 10.000.000 € fino al 2% del fatturato mondiale

Art.8 privacy dei minori

Art.11 (? forse 10 dati giudiziari)

Artt.25-39

Privacy by design e by default
Contitolari del trattamento
Titolari non UE
Responsabile del trattamento
Registro delle attività di trattamento
Cooperazione con l'autorità di controllo
Sicurezza del trattamento
Comunicazione della violazione
PIA
Responsabile della protezione dei dati
Certificazione

Capo VIII Sanzioni
20.000.000 € fino al 4% del fatturato mondiale

Art.5 trattamento dei dati

Art.6 liceità del trattamento

~~Art.7 consenso al trattamento~~

~~Art.9 trattamento di dati genetici, di salute, razziali, orientamento sessuale~~

Art.13 informativa

Art.15 diritto di accesso

~~Art.16 diritto di rettifica~~

~~Art.17 diritto di cancellazione~~

~~Art.18 diritto di limitazione~~

Art.20 diritto alla portabilità

Capo VIII Sanzioni
20.000.000 € fino al 4% del fatturato mondiale

Art.44-49 trasferimento dei dati in un paese terzo
Inosservanza di un ordine dell’autorità di controlo

La normativa Europea sulla privacy

In sintesi

Consenso dell’interessato: non è necessario. Se si fa firmare un modulo deve essere semplice, chiaro, non mescolato ad altri moduli, etc ...

La normativa Europea sulla privacy

In sintesi

Informativa: può essere appesa in sala d’attesa e deve riportare I dati di cui all’art.13

La normativa Europea sulla privacy

In sintesi

Responsabile del trattamento
Responsabile della protezione

Non sono obbligatori
Se si nominano serve un contratto scritto

La normativa Europea sulla privacy

In sintesi

PIA = DPS
Non dovrebbe essere obbligatoria
(ma alla fine cosa ci costa? Facile!)

La normativa Europea sulla privacy

In sintesi

Registro dei trattamenti
Non dovrebbe essere obbligatoria
(ma alla fine cosa ci costa? Facile!)

La normativa Europea sulla privacy

In sintesi

Incaricati dei trattamenti: formazione

La normativa Europea sulla privacy

In sintesi

Consenso dell’interessato: no
Informativa: si
Responsabile del trattamento: no
Responsabile della protezione: no
PIA: no?
Registro dei trattamenti: no?
Incaricati dei trattamenti: formazione

La normativa Europea sulla privacy

Grazie per l’attenzione