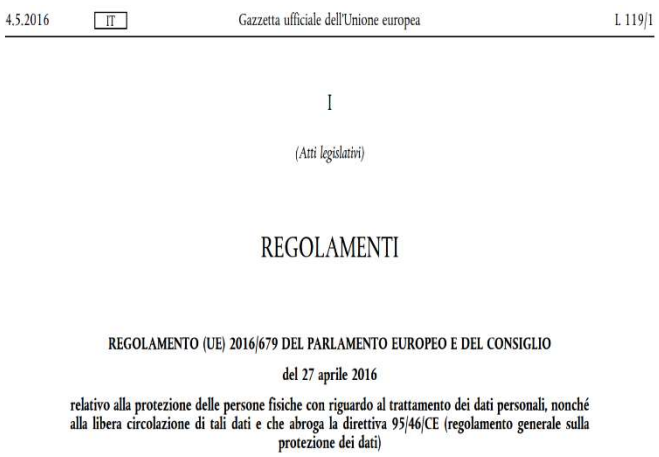


4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/1

I

(Atti legislativi)

REGOLAMENTI

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 (regolamento generale sulla protezione dei dati)

Azienda Ospedaliero Universitaria delle Marche

REGOLAMENTO UE 2016/679: RISPETTO DELLA RISERVATEZZA DEI DATI

Ancona, 21 novembre 2023

Marianna Catalini
Responsabile per la protezione dei dati

Azienda Ospedaliero Universitaria delle Marche

AMBITO DI APPLICAZIONE:

Il Regolamento <u>si applica:</u>

- solo al trattamento dei dati relativi a <u>persone fisiche</u> = *«interessato» che si trovi nell'UE, a prescindere dalla nazionalità o dal luogo di residenza (c.14);*

*È **<u>interessato</u>** la persona fisica del quale i dati personali sono trattati*



Il Regolamento <u>non</u> <u>si applica (art. 2, co.2):</u>

- ai dati personali relativi a <u>persone giuridiche</u>, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto (c.14) = la ragione è la persona fisica è soggetto che necessità di maggior protezione

- ai trattamenti di dati personali effettuati da una persona fisica per <u>attività di carattere esclusivamente personale o domestico</u> (….) = siamo al di fuori dall'ambito delle relazioni commerciali

- <u>ai dati anonimi</u>

IL REGOLAMENTO È BASATO SUL PRINCIPIO DI ACCOUNTABILITY: *responsabilizzazione*

Questa consiste nell'obbligo per il titolare del trattamento di adottare **misure appropriate ed efficaci** per attuare i principi di protezione dei dati, nonché nella necessità di **dimostrare, su richiesta,** che sono state adottate misure appropriate ed efficaci.

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.

DEFINIZIONI ESSENZIALI:

- **DATO PERSONALE:** qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato)

- **TRATTAMENTO:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali

- **TITOLARE**: "titolare" è la persona fisica o giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le scelte di fondo sulle finalità e sulle modalità del trattamento dei dati, anche per ciò che riguarda la sicurezza.

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**".

il rapporto tra titolare del trattamento e responsabile del trattamento deve essere **disciplinato da un accordo** tra le parti il cui contenuto minimo è definito.

RESPONSABILE DEL TRATTAMENTO

Il Regolamento ha lasciato la facoltà alle organizzazioni di **nominare dei soggetti interni che supportano nella gestione delle attività di trattamento** il Titolare negli ambiti di loro competenza.

La nomina qualora effettuata deve prevedere **le istruzioni che devono essere chiare, coincise, sintetiche ma efficaci** ai fini del perseguimento delle finalità che il titolare si prefisse in applicazione del principio di responsabilizzazione

Per le modalità di individuazione e nomina dei responsabili interni il Regolamento comunitario **lascia ampia libertà di scelta** al Titolare del trattamento in ragione della peculiarità organizzativa propria di ogni organismo

RESPONSABILE PROTEZIONE DATI
DATA PROTECTION OFFICER - DPO

Figura indipendente nominata da titolare e dal responsabile del trattamento

Informa e consiglia

Sorveglia

Fornisce un parere sulla valutazione d'impatto sulla protezione dei dati (PIA) e ne sorveglia lo svolgimento

E' punto di contatto e collabora l'Autorità di controllo

Valuta i rischi del trattamento, considerandone la natura, il campo di applicazione, il contesto e le finalità

Figura di vigilanza, interna o esterna

Designato in base a qualità professionali

E' coinvolto in tutte le questioni

Non deve ricevere istruzioni e non dev'essere in conflitto d'interessi

OBBLIGATORIO PER

Pubbliche amministrazioni e organismi pubblici

Soggetti che effettuano un controllo regolare e sistematico degli interessati su larga scala

Soggetti che trattano, su larga scala, dati particolari

IL REGOLAMENTO È DEFINISCE ALCUNI PRINCIPI GENERALI:

Principio	Significato
LICEITÀ, CORRETTEZZA E TRASPARENZA	Dati trattati in modo lecito, corretto e trasparente nei confronti dell'interessato
LIMITAZIONE DELLA FINALITÀ	Dati raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità oppure comunque a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici
MINIMIZZAZIONE DEI DATI	Dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati
ESATTEZZA	Dati 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

IL REGOLAMENTO È DEFINISCE ALCUNI PRINCIPI GENERALI:

Principio	Significato
LIMITAZIONE DELLA CONSERVAZIONE	Dati 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 se trattati esclusivamente ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici
INTEGRITÀ E RISERVATEZZA	Dati trattati in modo da garantire un'adeguata sicurezza , compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

EVENTI DA PREVENIRE…

Comportamenti degli operatori	• Sottrazione di credenziali di autenticazione • Carenza di consapevolezza, disattenzione o incuria • Comportamenti sleali o fraudolenti • Errore materiale
Eventi relativi agli strumenti	• Azione di virus informatici o di programmi che possono arrecare danno • Spamming o tecniche di sabotaggio • Malfunzionamento o deterioramento degli strumenti • Accessi esterni non autorizzati • Intercettazione di informazioni in rete
Eventi relativi al contesto	• Accessi non autorizzati a locali • Sottrazione di strumenti contenenti dati • Eventi distruttivi, naturali o artificiali, dolosi o accidentali o dovuti a incuria • Guasto a sistemi complementari • Errori umani nella gestione della sicurezza fisica

ALCUNE MISURE DI SICUREZZA

Adozione misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

- ✓ **Pseudonomizzazione**
- ✓ **Cifratura dei dati**
- ✓ **Riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento**
- ✓ **Capacità di ripristinare la disponibilità e l'accesso dei dati in seguito ad incidente**
- ✓ **Procedura per valutare l'efficacia delle misure tecnico ed organizzative per la sicurezza del trattamento**

PROCEDURA DATA BREACH

Adozione di procedure tecniche – organizzative finalizzate alla gestione della violazione dei dati personali prevedendo i criteri per le comunicazioni obbligatorie

VALUTAZIONE DI IMPATTO

Adozione procedura di valutazione dell'impatto dei trattamenti sulla protezione dei dati personali anche per adozione di nuove tecnologie.

RAPPORTO CON L'INTERESSATO

INFORMATIVA

Contenuti

- Riferimenti titolare trattamento e RPD
- Finalità e base giuridica del trattamento
- Destinatari del trattamento
- Categorie di dati
- Il periodo di conservazione
- I diritti degli interessati
- Obbligo o facoltatività del trattamento

RAPPORTO CON L'INTERESSATO

CONSENSO

Base di liceità del trattamento

Consenso espresso dell'interessato con indicazione delle finalità del trattamento

Le altre….

- Contratto
- Obbligo legale
- Salvaguardia di interessi vitali
- Compito di interesse pubblico o connesso all'esercizio di pubblici poteri
- Perseguimento interesse legittimo del titolare

COMUNICARE / DIFFONDERE

COMUNICAZIONE:

portare a conoscenza un soggetto ben identificato di una informazione (mail, lettera, telefonata etc.)

DIFFUSIONE

portare a conoscenza una pluralità di soggetti non facilmente identificabili di una informazione.(giornale, internet, affissione pubblica etc.)

ESEMPI…

FOTO SMARTPHONE TABLET	Non è mai lo scatto della foto (o la ripresa video/registrazione audio) ad essere messo in discussione, bensì l'uso che ne viene fatto. E' sempre possibile eseguirle anche senza il consenso delle persone presenti, purché l'uso che ne seguirà sia strettamente personale (ambito familiare, amicale). Attenzione alla loro pubblicazione su social network, pubblicazioni, ecc. poiché in quel caso occorre chiedere il consenso ai presenti.
CHIAVETTE USB	La semplice custodia di dati personali costituisce un vero e proprio «trattamento». Tenere in tasca o in borsa una chiavetta USB con informazioni personali espone a responsabilità in caso di smarrimento Non dimenticate che si può acquistare una chiavetta criptata o con accesso biometrico che ci risolve il problema.

ESEMPI…

VIDEO SORVEGLIANZA	per fini di tutela dei beni, è possibile installare telecamere purché: la presenza sia segnalata accordo sindacale o autorizzazione da parte dell'ispettorato del lavoro se sono esterne il loro angolo di visuale sia delimitato le immagini registrate siano distrutte entro 24 ore, salvo eccezioni

IN OSPEDALE…

- ✓ **Dati anamnestici**
- ✓ **Diagnosi**
- ✓ **Prescrizione di accertamenti**
- ✓ **Informazioni relative ad altri pazienti**
- ✓ **Informazioni relative a familiari e visitatori**

SANZIONI

- ✓ DISCIPLINARI
- ✓ AMMINISTRATIVE
- ✓ PENALI

ma ciò che si rischia in conseguenza ad una violazione della privacy è **la loro conseguenza civile** cioè il:

RISARCIMENTO DANNI

CONCLUSIONI

Nella Carta dei diritti fondamentali dell'Unione europea, il diritto alla protezione dei dati è ***collocato proprio nella parte riguardante la libertà****.*
[…]
La forte tutela dei dati sensibili è divenuta una componente essenziale dell'eguaglianza, per evitare che la raccolta di queste particolari informazioni possa trasformarsi in uno strumento di discriminazione delle persone. ***Ma la tutela dei dati sanitari o genetici è anche la condizione per realizzare il diritto alla salute****, così come la tutela dei dati sulle opinioni diventa una premessa per esercitare la libertà di espressione, comunicazione, associazione, culto.*

Stefano Rodotà