REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI

(Regolamento UE 2016/679 del parlamento Europeo e del Consiglio del 27,04,2016)

sintesi per CCM 28.06.2018

Ufficio Privacy Azienda Ospedaliero-Universitaria di Bologna Policlinico S. Orsola-Malpighi

La normativa di riferimento

Il **Regolamento Europeo (n.679/2016)** è diventato direttamente applicabile il **25 maggio 2018**

E' entrato in vigore il 24,05,2016, ha sostituito il Codice in Materia di Protezione dei Dati Personali (D.Lgs. 30 giugno 2003 n. 196) che derivava dalla **Legge sulla Privacy** (Legge 31 dicembre 1996, n. 675) che attuava la **Direttiva Comunitaria 95/46/CE**

In pratica diritto alla privacy è:

- ✓ diritto di essere informati sui trattamenti dei dati che ci riguardano e sulle relative finalità del trattamento

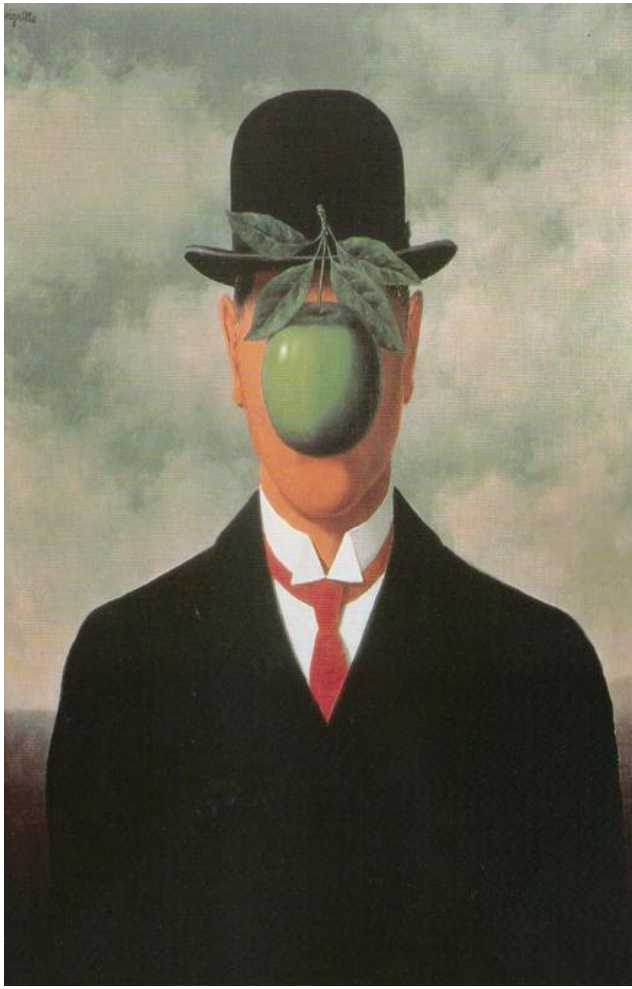
- ✓ diritto di scelta circa l'uso che vogliamo gli altri facciano dei nostri dati, attraverso l'espressione del consenso in diverse circostanze

- ✓ diritto di controllo sul trattamento dei dati svolto da soggetti terzi

Chi è il **Garante Privacy?**

Il **GARANTE per la protezione dei dati personali** è

- ✓ un'**autorità amministrativa indipendente** dotata di **poteri ispettivi e di indagine, sanzionatori, decisori e regolamentari**
- ✓ un **organo collegiale** composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile.



LE PRINCIPALI NOVITA’

- ✓ contiene **meno adempimenti formali**

- ✓ **privilegia aspetti sostanziali** come la valutazione dei rischi su cui costruire idonee misure di sicurezza, il principio della responsabilizzazione, la valutazione dell’impatto del trattamento sulla protezione dei dati, impone che l'utente sia informato in modo trasparente su come sono trattati i suoi dati personali in modo conciso e con un linguaggio chiaro e di semplice comprensione.

- ✓ Questo significa che le aziende non potranno più trattare la privacy come una mera questione burocratica e avranno l'incombenza di redigere informative giuridicamente valide evitando però un gergo strettamente legalese che ne potrebbe inficiare la validità con il rischio di essere sanzionate

STRUMENTI per una migliore qualità al fine del rispetto delle norme in materia di protezione dei dati

Adozione di una serie di MISURE intese ad aumentare la responsabilità dei Responsabili del trattamento

Adozione di MISURE DI SICUREZZA compreso l'obbligo di comunicare le violazioni dei dati personali

Identificazione di un **RESPONSABILE DELLA PROTEZIONE DEI DATI** (RPD – DPO) incaricato di garantire il rispetto delle norme.

SINTESI del NUOVO CONTENUTO (I)

TRATTAMENTI

- ✓ CONSENSO: effettivo ed equivocabile, scritto o verbale
- ✓ VALUTAZIONE DI IMPATTO: in casi specifici come il ricorso a tecnologie a rischio per i diritti alla persona il trattamento deve essere testato con una valutazione di impatto ed eventualmente con una consultazione preventiva del garante
- ✓ PRIVACY BY DESIGN: il regolamento impone di progettare sistemi e applicativi tarati sul principio dell'uso minimo e indispensabili dei dati personali
- ✓ PRIVACY BY DEFAULT: il regolamento impone di progettare misure e sistemi che abbiano come impostazione predefinita solo l'uso dei soli dati necessari per una certa finalità
- ✓ SICUREZZA: sul titolare incombe l'obbligo di effettuare l'analisi dei rischi e di vaglio dell'adeguatezza delle misure di tutela
- ✓ VIOLAZIONE DEI DATI: si estende a tutti la regola delle notifica di violazione al garante e all'interessato
- ✓ DATA PROTECTION OFFICER: nuova figura di riferimento interfaccia con garante
- ✓ REGISTRI TRATTAMENTI: il titolare ed il resp devono redigere i registri di competenze in cui indicare le caratteristiche, modalità, e finalità dei trattamenti
- ✓ CODICI ETICI E CERTIFICAZIONI: codici di autoregolamentazione e ricorso alle certificazioni dei trattamenti sono incoraggiati

DIRITTI:

- ✓ PORTABILITA' DEI DATI: all'interessato viene riconosciuto il diritto di ottenere la restituzione dei propri dati personali trasmessi ad un'azienda o un servizio on line e trasmetterli ad altri
- ✓ OBLIO: il regolamento codifica il diritto dell'interessato di chiedere ai motori di ricerca di deindicizzare una pagina web o chiedere ad un sito web di codificare informazioni
- ✓ PROFILAZIONE: il regolamento sancisce il diritto a non subire profilazioni inconsapevoli
- ✓ SPORTELLO UNICO: l'interessato può rivolgersi all'autorità di protezione dei dati del proprio paese per segnalare eventuali violazioni

SANZIONI

PECUNIARIE AMMINISTRATIVE: calcolate anche in misura percentuale (dal 2 al 4%) sul fatturato globale annuo mondiale

AUTORITA'

- ✓ COMITATI DI CONTROLLO EUROPERO: organo europeo che assicura l'applicazione uniforme del regolamento
- ✓ AUTORITA' DI CONTROLLO: autorità pubblica indipendente istituita da uno stato membro. Il codice privacy italiano definisce il garante per la protezione dei dati personali

Un po' di DEFINZIONI utili

- ✓ Le categorie dei **DATI PERSONALI**
  - ⇨ **Dato identificativo**
  - ⇨ **Dato sensibile /relativo alla salute**
  - ⇨ **Dato genetico**
  - ⇨ **Dato giudiziario**
  - ⇨ **Dato anonimo**
- ✓ Cosa si intende per **TRATTAMENTO dei dati personali**
- ✓ Quali sono i **SOGGETTI** coinvolti nel trattamento dei dati
  - ⇨ **Interessato**
  - ⇨ **Titolare del trattamento**
  - ⇨ **Soggetto delegato**
    ex Resp.del trattamento
  - ⇨ **Addetto al trattamento**
    ex Incaricato del trattamento

Le categorie dei DATI PERSONALI

DATO PERSONALE:

qualunque informazione relativa a persona fisica IDENTIFICATA o IDENTIFICABILE, anche indirettamente, mediante riferimento a qualsiasi altra informazione (es. dati anagrafici, indirizzo, numero di telefono, cellulare, codice fiscale, matricola, tessera sanitaria, dati biometrici, impronte digitali, immagini, audio...)

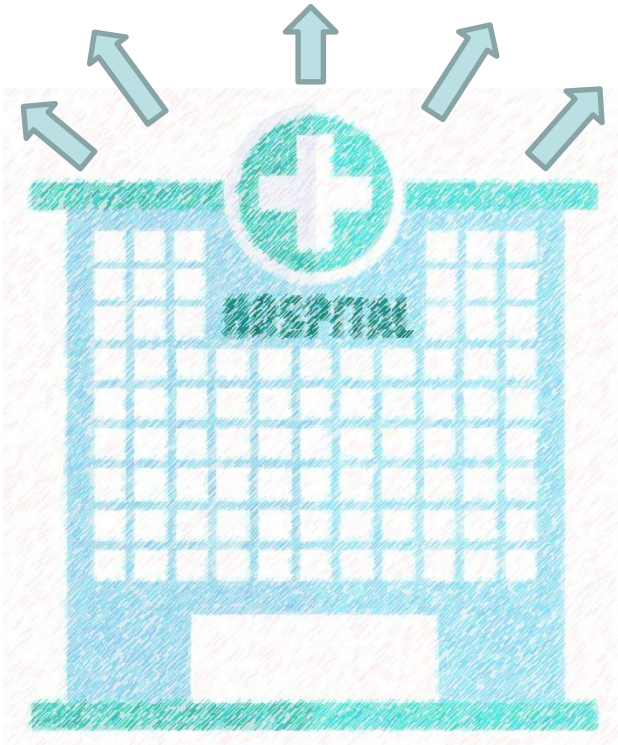
- ✓ **Dato identificativo**: dato personale che permette l'identificazione diretta di un soggetto (dati anagrafici, le immagini, ecc.);
- ✓ **Dato relativo alla salute**: dato personale attinente alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rivelano informazioni relative al suo stato di salute
- ✓ **Dato genetico:** dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono indicazioni 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
- ✓ **Dato giudiziario**: dato personale idoneo a rivelare provvedimenti 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 artt. 60 e 61 del C.P.P.
- ✓ **Dato anonimo**: dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile

Il TRATTAMENTO dei dati personali

Per trattamento s'intende (ex art 4 Cod. Privacy) **qualunque operazione** o complesso di operazioni, effettuate sui dati, anche senza l'ausilio di strumenti elettronici e anche se non registrati in una banca di dati, concernenti

- ✓ raccolta
- ✓ registrazione
- ✓ organizzazione
- ✓ conservazione
- ✓ consultazione
- ✓ elaborazione
- ✓ modificazione
- ✓ selezione
- ✓ estrazione
- ✓ raffronto
- ✓ utilizzo
- ✓ interconnessione
- ✓ blocco
- ✓ cancellazione
- ✓ distruzione

- ✓ comunicazione
- ✓ diffusione



I SOGGETTI coinvolti nel trattamento dei dati

Le figure coinvolte nella tutela dei dati sono:

- ✓ **INTERESSATO**
- ✓ **TITOLARE** del trattamento
- ✓ **SOGGETTO DELEGATO a**l trattamento
- ✓ **AUTORIZZATO a**l trattamento

INTERESSATO

la persona fisica cui si riferiscono i dati personali

PROPRIETARIO dei DATI

soggetto centrale dell'intero quadro normativo

quindi, nel nostro ambito di interesse **il paziente**

I diritti dell'interessato

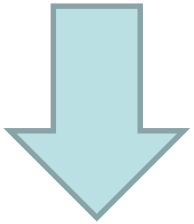
All'interessato il Regolamento riconosce una serie di **diritti** e prerogative tutte relative all'effettività dell'esercizio del controllo sulla circolazione dei propri dati personali che si compiono con l'applicazione di un gruppo di norme a presidio della tutela prescritta

- ✓**ACCESSO**
- ✓**RETTIFICA E CANCELLAZIONE**
- ✓**LIMITAZIONE AL TRATTAMENTO**
- ✓**PORTABILITA' DEI DATI**
- ✓**OPPOSIZIONE**

I diritti dell'interessato sono esercitati con **richiesta rivolta senza formalità** (lettera, fax, mail..) al Titolare o al Responsabile, anche per il tramite di un incaricato, alla quale è fornito **idoneo riscontro senza ritardo**

TITOLARE del trattamento

persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza



l'**Azienda** nella persona del **Direttore Generale**

SOGGETTO DELEGATO

soggetto preposto dal Titolare al trattamento dei dati personali, scelto tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia circa il rispetto delle disposizioni vigenti in materia di tutela dei dati personali, ivi compreso il profilo della sicurezza

Si tratta di una nomina:

- ✓ facoltativa
- ✓ scritta che specifica analiticamente i compiti affidati dal Titolare

all'interno della nostra Azienda vengono nominati Soggetti delegati

- ✓ **Direttori di UO**
- ✓ **Responsabili di UO, SSD, Programmi**
- ✓ **Coordinatori infermieristici/tecnici e della riabilitazione**

cosa comporta essere Soggetto delegato?

Il Soggetto del trattamento assume, con la nomina, una **responsabilità diretta** rispetto al trattamento dei dati cui è preposto. In particolare lo stesso è tenuto a:

- ✓ osservare le istruzioni e le misure di sicurezza indicate dal Titolare nell'atto di nomina
- ✓ verificare periodicamente lo stato di applicazione del R.E, anche in relazione alle indicazioni del Garante per la protezione dei dati personali
- ✓ rivisitare, alla luce degli obblighi imposti dalla normativa, le procedure esistenti all'interno del proprio Servizio/Struttura/UO
- ✓ designare gli incaricati del trattamento, impartendo loro idonee istruzioni, e vigilare sul rispetto delle stesse ⇨ **N.B.** il soggetto delegato ha il dovere di conservare ai propri atti l'**elenco degli autorizzati** munito di firme sempre aggiornato!
- ✓ assicurare la partecipazione degli incaricati agli aggiornamenti formativi in materia, incentivando lo sviluppo di una «cultura privacy» nel proprio ambito di afferenza

AUTORIZZATO del trattamento

persona fisica autorizzata dal Titolare o dal Soggetto delegato, tramite nomina, a compiere le operazioni di trattamento. Dunque operativamente l'autorizzato è colui che quotidianamente compie operazioni di trattamento di dati, sia su supporto cartaceo, che su supporto informatico

Pertanto, la lettura combinata degli strumenti sopra citati consente di poter individuare l'ambito del trattamento assegnato a ciascun incaricato. Infatti da un lato i documenti aziendali individuano le attività ed i profili di autorizzazione delle varie figure professionali, dall'altro le assegnazioni degli incaricati sono documentate per iscritto.

Si tratta di una nomina:

- ✓ obbligatoria
- ✓ scritta che deve contenere istruzioni puntuali e definire l'ambito del trattamento posto in essere dall'Incaricato → FORMAT AZIENDALE
- ✓ minima di sicurezza per ogni Azienda

all’interno dell’Azienda devono essere nominati autorizzati TUTTI i **dipendenti** che trattano dati ad esempio:

- ✓ *amministrativi*
- ✓ *infermieri, tecnici sanitari e personale riabilitazione*
- ✓ *medici*
- ✓ *personale ruolo professionale, ruolo tecnico e di vigilanza*
- ✓ …

Informativa e Consenso

Gli organismi sanitari pubblici e privati (ospedali, case di cura...), come pure gli esercenti le professioni sanitarie (farmacisti, medici, infermieri..) hanno l'**OBBLIGO** di fornire al paziente un'informativa sul trattamento dei dati personali che lo riguardano e di acquisire il consenso al loro uso.

L' INFORMATIVA

- ✓ è lo strumento che rende esplicita e trasparente la gestione delle informazioni di carattere personale e/o sensibile degli interessati.

- ✓ Deve essere fornita all'Interessato **prima** ⇨ di effettuare il trattamento dei suoi dati
  ⇨ di acquisire il relativo consenso

- ✓ La mancanza di informativa o la carenza del suo contenuto causa l'invalidità del consenso eventualmente ottenuto

- ✓ Può essere ⇨ scritta (preferibile)
  ⇨ orale

- ✓ Rientra nella discrezionalità degli organismi sanitari predisporre alternativamente :
  ⇨ unica informativa
  ⇨ pluralità di informative ⇨ in relazione a una pluralità di prestazioni erogate da diversi reparti o strutture ospedaliere o territoriali.

- ✓ La struttura che ha reso l'informativa deve attestare di averla fornita con modalità uniformi e con adeguate misure organizzative che ne consentano la verifica (es. modalità di rilascio orale con evidenza della codificazione di un'informativa aziendale esposta in formato locandina e facilmente visibile al pubblico, ad es. presso sale d'attesa).

Il CONSENSO

- ✓ è l'**autorizzazione** a trattare i dati personali e clinici del paziente e costituisce la legittimazione al trattamento dei dati. Il sanitario è infatti tenuto a rispettare il diritto alla riservatezza su tutte le informazioni riguardanti la sfera personale e «sensibile» della persona, sicché **non** potrà trattare nessun dato del paziente senza il suo consenso

- ✓ il consenso dell'Interessato deve essere
  - ⇨ informato
  - ⇨ specifico
  - ⇨ libero
  - ⇨ inequivocabile

- ✓ il consenso può essere manifestato in forma:
  - ⇨ **scritta,** mediante sottoscrizione di apposito modulo
  - ⇨ **orale**, purché documentato per iscritto o annotato informaticamente
  - ⇨ di **unica dichiarazione** ovvero non deve necessariamente essere richiesto caso per caso, ma anche una volta soltanto il relazione all'insieme delle attività che verranno esplicate nei confronti dell'interessato.

Chi è legittimato a manifestare il consenso?

Interessato: maggiorenne, non interdetto, capace di intendere e volere

Delegati per legge a prestare il consenso per l'interessato incapace o impossibilitato ovvero i **Rappresentanti Legali** dell'interessato interdetto, inabilitato o minorenne:

- ✓ Tutore, Curatore, Amministratore di sostegno
- ✓ Esercente la responsabilità genitoriale

In mancanza di questi ultimi:

- ✓ Prossimo congiunto
- ✓ Familiare
- ✓ Convivente
- ✓ Responsabile della struttura presso cui dimora l'interessato

FASCICOLO SANITARIO ELETTRONICO (FSE)

è uno **strumento**:

✓di raccolta e gestione di dati sanitari del paziente, relativi ad eventi clinici presenti e trascorsi, originati da **molteplici titolari di trattamento** *ovvero*

⇨ da soggetti che, a vario titolo, prendono in cura il paziente nell'ambito del SSN e dei servizi socio-sanitari regionali (es. MMG/PLS, strutture pubbliche SSR (es. AUSL, AOSP) e strutture private accreditate) che lo alimentano in maniera continuativa

✓regionale: in Emilia Romagna il FSE è gestito da Cup2000

Fascicolo Sanitario elettronico
Regione Emilia-Romagna

✓costituito per finalità di prevenzione, diagnosi, cura e riabilitazione perseguite dai soggetti del SSN e dei servizi sociosanitari regionali che prendono in cura l'assistito

⇨ quindi costituisce la storia clinica «regionale» del paziente

✓facoltativo che può essere attivato dal paziente, attraverso raccolta di apposito consenso rivolgendosi al gestore Cup2000

✓a cui ha accesso ⇨ il paziente

⇨ MMG / PLS **solo** se espressamente autorizzato dal paziente

DOSSIER SANITARIO ELETTRONICO (DSE)

è uno **strumento**:

- ✓ di raccolta e gestione di dati sanitari del paziente, relativo ad eventi clinici presenti e trascorsi, originati da un **unico titolare del trattamento** *ovvero*

  ⇨ da un unico organismo sanitario al cui interno operano diversi professionisti

- ✓ aziendale: nella nostra Azienda DSE è l'applicativo GALILEO e-HEALTH SOLUTIONS

- ✓ costituito per finalità di prevenzione, diagnosi, cura e riabilitazione perseguite dall'Azienda ⇨ quindi costituisce la storia clinica «aziendale» del paziente

- ✓ facoltativo. I professionisti aziendali sono preposti alla raccolta del consenso del paziente alla costituzione o meno al DSE

- ✓ a cui ha accesso **solo** il medico dell'Azienda che ha in cura il paziente

Le regole in azienda

- ✓ applicazione del Regolamento sulla protezione di dati personali → **IOA29**
- ✓ regolamento aziendale in tema di sicurezza e riservatezza nell'uso delle risorse informatiche → **IOA44**
- ✓ istruzione operativa aziendale per l'utilizzo della posta elettronica e di internet → in fase di emissione
- ✓ richiesta di copia della cartella clinica e di altra documentazione sanitaria → **PA36**
- ✓ archiviazione e smaltimento della documentazione aziendale → **PA40**

Dove trovare la documentazione?

nell'area **Documentazione Aziendale**:
tutta la documentazione aziendale (IOA, tabelle, report…)

nell'area **Privacy**:

- ✓ Documentazione del Garante Privacy
- ✓ Documentazione aziendale