GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Il nuovo REGOLAMENTO EUROPEO sulla protezione dei dati

(**G**eneral **D**ata **P**rotection **R**egulation)

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

18.04.2019 e 21.11.2019

PROGRAMMA

- ✓ Le principali novità del Regolamento
- ✓ Principali riferimenti normativi
- ✓ Principali definizioni
- ✓ Ambito di applicazione e principi
- ✓ Attori coinvolti
- ✓ I diritti dell'interessato
- ✓ Adempimenti di un titolare: misure tecniche ed organizzative

- ✓ Analisi di un caso

Pausa

- ✓ Cenni sulla sicurezza informatica del dato
- ✓ L'autorità di controllo
- ✓ Reclamo all'Autorità Garante
- ✓ Il sistema sanzionatorio

Test finale

OBIETTIVO

Illustrare le principali novità e caratteristiche della nuova normativa al fine di fornire le indicazioni per il soddisfacimento «sostanziale» degli adempimenti richiesti

LA PRIVACY E LA RISERVATEZZA

Il concetto di **riservatezza** ha conosciuto nel tempo origini, evoluzioni e fortune differenziate nei diversi paesi del mondo.
Il significato di diritto alla *privacy* può definirsi come il **diritto di ogni individuo a essere lasciato in pace, libero da interferenze nella propria vita privata**.
In Italia, l'esistenza di un vero e proprio diritto alla riservatezza, è stato a lungo dibattuto. Con l'entrata in vigore nel 2009 del Trattato di Lisbona, nella Carta dei diritti fondamentali dell'Unione europea del 2000 (nota anche come Carta di Nizza) il diritto alla riservatezza ha assunto il medesimo valore giuridico dei trattati ed è vincolante per gli Stati membri.

Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni (art. 7 carta di Nizza)

Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
***Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*"** (art. 8).

Nel tempo, con l'evolvere e l'espandersi delle tecnologie dell'informazione, il **concetto di *privacy*** ha acquisito una connotazione settoriale più marcata: **si tratta del diritto del singolo anche a controllare l'uso che altri potrebbero fare di informazioni riguardanti sé stesso**.

IN PRATICA DIRITTO ALLA PRIVACY È:

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

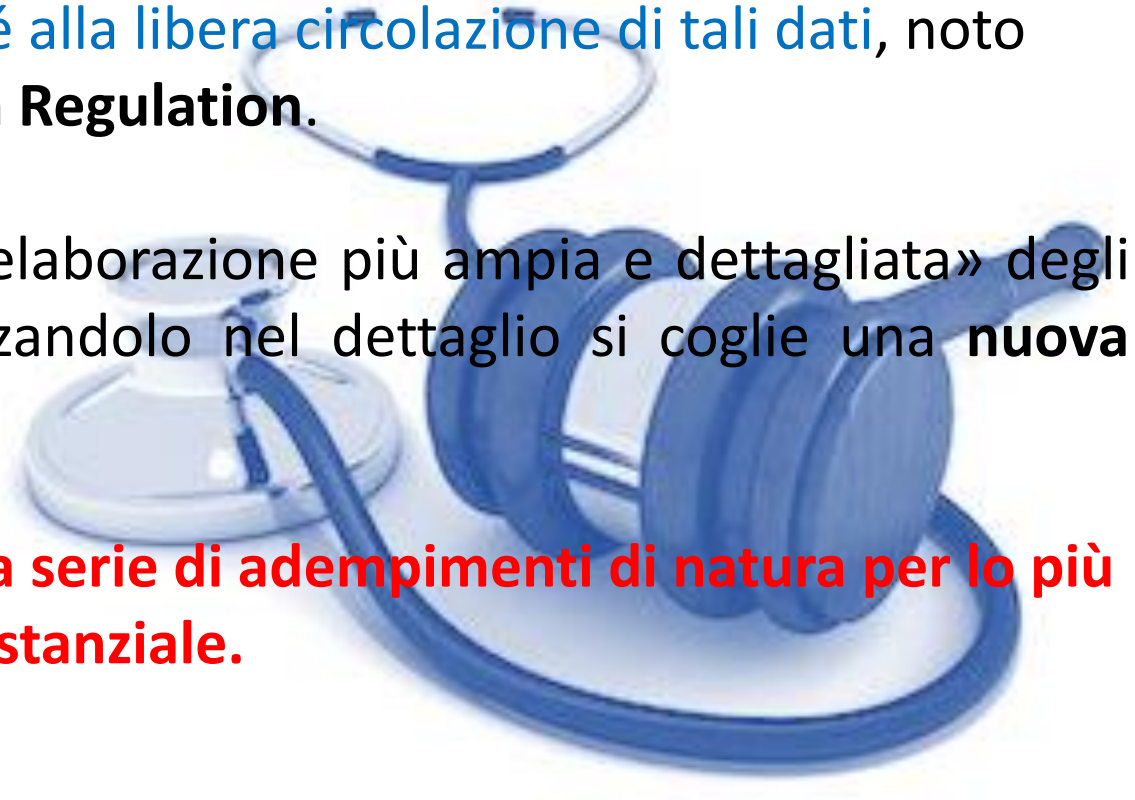
- ✓ diritto di scelta circa l'uso che vogliamo gli altri facciano dei nostri dati, attraverso l'espressione del consenso in diverse circostanze

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

IL PANORAMA NORMATIVO: come ci si è arrivati

Dopo un lungo iter legislativo, il 14 aprile 2016 il Parlamento Europeo, al fine di definire e garantire, in materia di protezione dei dati personali, un sistema armonizzato e un **quadro giuridico comune per tutti gli Stati membri dell'Unione Europea**, ha definitivamente approvato il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, noto come **GDPR** acronimo di **General Data Protection Regulation**.

Nonostante il nuovo RE possa sembrare una «rielaborazione più ampia e dettagliata» degli stessi principi della Direttiva 95/46/CEE, analizzandolo nel dettaglio si coglie una **nuova filosofia:**



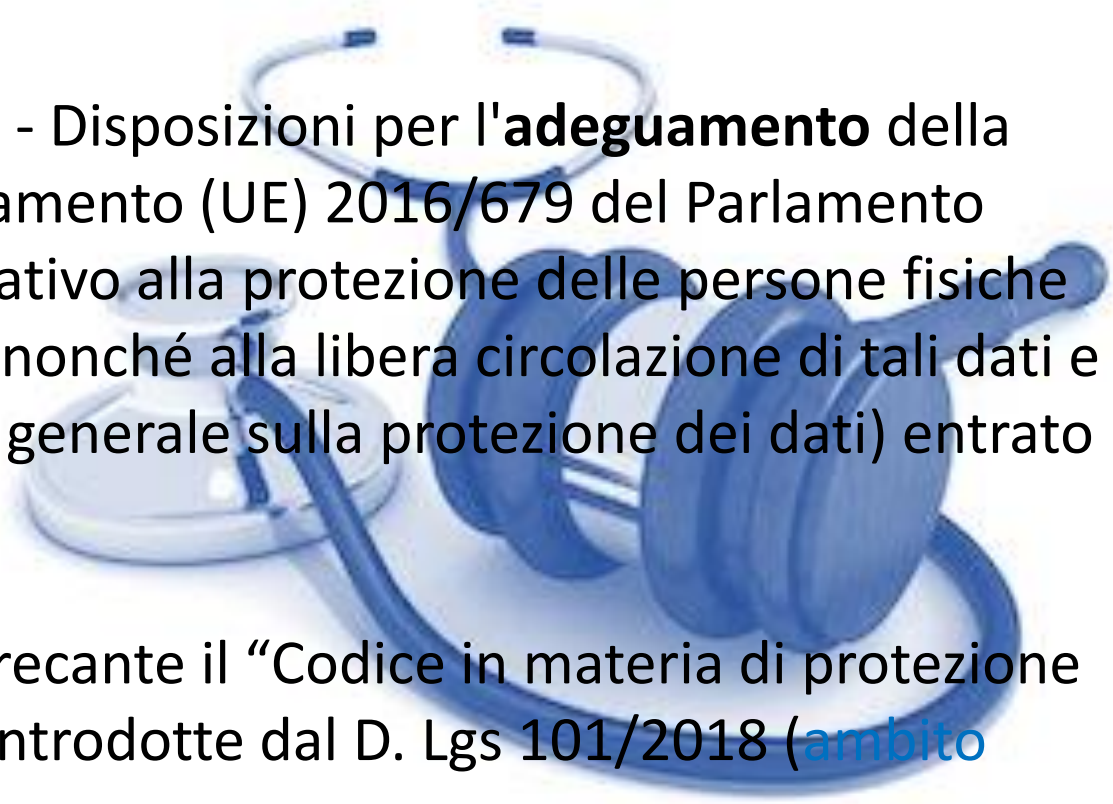
il passaggio da una disciplina che raccoglieva una serie di adempimenti di natura per lo più formale, ad un quadro normativo fortemente sostanziale.

IL PANORAMA NORMATIVO

- ✓ **REGOLAMENTO EUROPEO** (2016/679) o GDPR (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali entrato in vigore il 24.05.2016, ma che si applica dal 25.05.2018 (ambito comunitario)

- ✓ **DECRETO LEGISLATIVO** 10 agosto 2018, n. 101 - Disposizioni per l'**adeguamento** della normativa nazionale alle disposizioni del 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) entrato in vigore il 19.09.2018 (ambito nazionale)

- ✓ **DECRETO LEGISLATIVO** 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" **integrato** con le modifiche introdotte dal D. Lgs 101/2018 (ambito nazionale)



IL PANORAMA NORMATIVO: il D. Lgs. 101/2018

DECRETO LEGISLATIVO 10 agosto 2018, n. 101
Provvedimento complesso sostanzialmente suddiviso in 2 parti: a) che va fino all'art. 16 relativa alle modifiche del Codice, b) relativa a tempi e modi di modifica degli atti emanati precedentemente.
Il Decreto salva i provvedimenti del garante e le autorizzazioni che saranno oggetto di successivo riesame e i Codici deontologici vigenti.

Introduce anche un periodo di 8 mesi circa in cui l'Autorità Garante adotterà particolari «attenzioni» nell'applicazione delle sanzioni tenendo conto che si tratta di una normativa nuova con sanzioni molto più elevate.

L'APPROCCIO del nuovo regolamento

Il RE rovescia completamente la prospettiva della disciplina sulla privacy istituendo un quadro normativo incentrato sui doveri e la responsabilizzazione del titolare del trattamento (**accountability**).

La nuova disciplina impone al titolare di **garantire il rispetto** dei principi in esso contenuto, ma anche di **essere in grado di comprovarlo** adottando una serie di **strumenti.** Occorre quindi partire da una attenta valutazione dei rischi e degli impatti e pianificare da subito le attività da realizzare che possono comportare modifiche culturali, organizzative e tecnologiche.

Il concetto di responsabilizzazione si traduce nel fatto che il titolare è chiamato a dimostrare che i trattamenti sono coerenti con il disposto del Regolamento, a pianificare e mettere in atto misure tecniche ed organizzative per poterne comprovare l'adeguatezza, ed ad attivare un modello di monitoraggio di tali misure.

L’APPROCCIO del nuovo regolamento

Nel nuovo assetto le scelte del Titolare del trattamento per una corretta tutela e protezione dei dati diventano un **cardine del sistema e misura della sua responsabilità**.

Secondo il principio dell’accountability il Titolare è competente per il rispetto della liceità, correttezza, trasparenza dell’intero trattamento dei dati e soprattutto è in grado di comprovarlo.

In altre parole il Titolare di una struttura sanitaria (pubblica o privata), non è più chiamato a provare e dimostrare una serie di adempimenti formali, ma il **rispetto sostanziale** dei principi base del sistema.

E’ evidente che in quest’ottica la nuova disciplina impone al titolare **un diverso approccio nel trattamento dei dati personali, prevedendo nuovi adempimenti, un’intensa attività di adeguamento e un forte impegno nel creare consapevolezza tra i professionisti sui principali requisiti del regolamento**.

GLI ATTORI: i soggetti coinvolti nel trattamento del dato

Interessato è la persona fisica alla quale si riferiscono i dati personali. Quindi, se un trattamento riguarda, ad esempio, l'indirizzo, il codice fiscale, ecc. di Mario Rossi, questa persona è l"interessato”

Titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento dei dati

Responsabile (esterno) è la persona fisica o giuridica, l’autorità pubblica, il servizio che tratta i dati per conto del titolare

GLI ATTORI: i soggetti coinvolti nel trattamento del dato

Personale autorizzato (ex INCARICATO): è il soggetto, persona fisica che adeguatamente formato dal titolare o altro soggetto da questo designato, effettua materialmente le operazioni di trattamento sui dati personali

Non è più presente la definizione della figura del responsabile interno, ma il Regolamento lascia libero il titolare di definire una figura analoga all'interno della propria struttura.

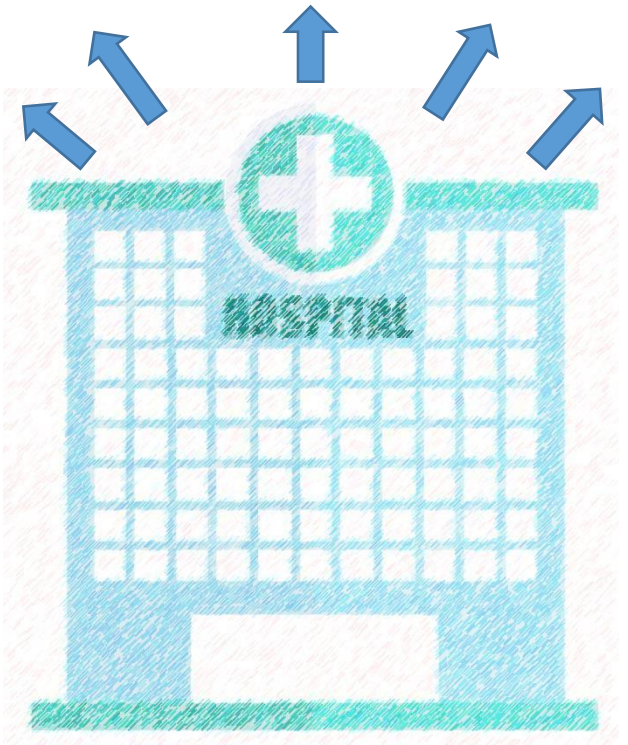
Responsabile della protezione dei dati (data protection officer –DPO)

è una figura nuova, obbligatoria in alcuni casi, ma sempre consigliata anche per i soggetti per i quali la nomina non è obbligatoria, deve avere caratteristiche ben definite che il regolamento definisce, può essere condiviso tra più titolari, in sintesi èè colui che deve vigilare sul trattamento dei dati di una struttura interfacciandosi con le autorità di controllo, è quindi una figura chiave importante per il titolare

Il TRATTAMENTO dei dati personali

Per trattamento s'intende **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

✓ comunicazione ✓ diffusione



Il TRATTAMENTO dei dati personali

COMUNICAZIONE: il dare conoscenza dei dati personali a uno o più soggetti DETERMINATI diversi dall'interessato, ……in qualunque forma, anche mediante la loro messa a disposizione, consultazione, o interconnessione.

DIFFUSIONE: il dare conoscenza dei dati personali a uno o più soggetti INDETERMINATI diversi dall'interessato, ……in qualunque forma, anche mediante la loro messa a disposizione, consultazione, o interconnessione.

Il dato: un nuovo concetto

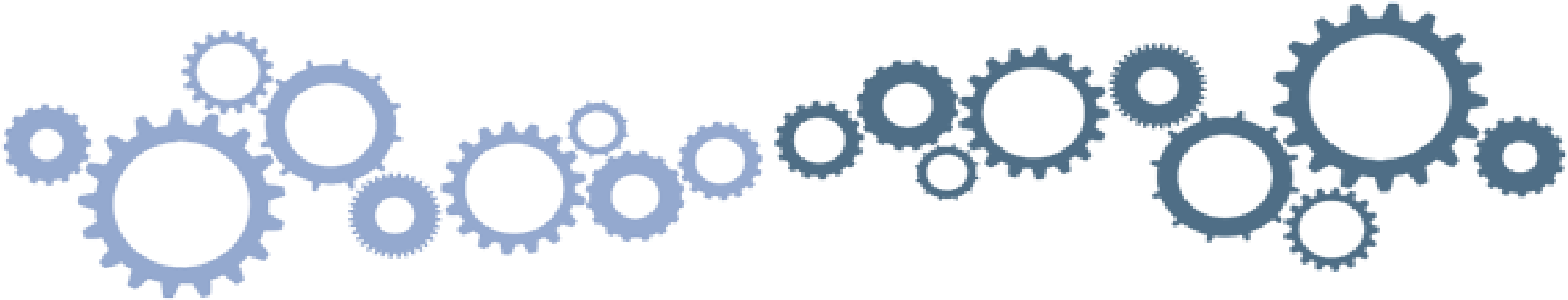
La nuova disciplina deve proteggere i dati e che consentire loro di circolare per creare ricchezza

E’ cambiato il contesto economico: oggi i dati sono digitali e sono la materia prima della nuova normativa (data economy)

«I DATI SONO IL MOTORE DELLA NUOVA ECONOMIA»

L'obiettivo della Commissione Europea è creare un mercato unico digitale, in cui la libera circolazione di merci, persone, servizi capitali e dati sia garantita e in cui i cittadini e le imprese possano accedere agevolmente e in modo equo a beni e servizi online, a prescindere dalla loro nazionalità o residenza….

..i dati saranno gli abilitatori della nuova sanità, la frontiera nella cura è la personalizzazione, dalle fasi della ricerca alla progettazione di nuovi farmaci… (Comunicato della Commissione Europea 25,05,2018)



Data dollar: i dati come moneta di scambio

Sapevamo di valere quindici dollari e novantotto centesimi? Questo è ciò che ciascun utente nel mondo vale per Facebook nel 2016. Gli statunitensi e i canadesi valgono molto di più: circa 63 dollari a utente. L'Europeo vale solo 19,4 dollari. Il primo trimestre 2017 però ha fatto segnare un incremento del 36% a pari periodo del 2016. Asia e Pacifico sono a 7,29 dollari e il "*resto del mondo*" arriva solo a 4,66 dollari.

Il valore commerciale dei dati personali

Questo patrimonio, in realtà, è il valore che hanno i nostri dati personali. L'apparente gratuità del *social network* non può fare a meno delle tracce di chi naviga, consuma, visualizza o clicca inserzioni. Senza i dati personali, il modello economico non regge, ogni dettaglio ha valore. Questo ha fatto sì che, nel febbraio di tre anni fa, Facebook abbia acquistato WhatsApp per circa 19 miliardi di dollari. All'epoca, la app aveva 465 milioni di utenti attivi. Oggi (dati al gennaio 2017) sono circa 1,2 miliardi. In Italia la diffusione è capillare: l'ultima rilevazione, risalente a novembre 2015, conta 20 milioni di utenti.

E la privacy?

La privacy non è più una prerogativa di istituzioni e governi democratici ma delle aziende tecnologiche. La privacy degli utenti è un **vincolo di fiducia** tra imprese tecnologiche e compratori. Io fornisco a te oggetti e/o servizi sempre più personalizzati, raccolgo i tuoi dati (che io azienda uso per profilazione e marketing, anche se con te utente non sarò completamente trasparente), cosicché **della tua vita solo io, azienda, so tutto: come il segreto bancario o quello medico.**

Scarsa consapevolezza

Il punto è che ancora ignoriamo quanto valore abbiano davvero i nostri dati. **Non diamo valore alle tracce di ciò che facciamo su Internet:** letture, navigazione e ricerca di siti su Google, acquisti su Amazon e controllo delle nostre abitudini di consumo attraverso il login, i like che diamo o riceviamo, la rubrica dei nostri contatti.

Da qui **Un esperimento provocatorio: i Data Dollar**

Data dollar: i dati come moneta di scambio

Data Dollar: una moneta che si basa sul valore dei dati personali diventa un nuovo metodo di pagamento

ICT

Mi piace 3 Condividi Tweet Share

Pubblicato il: 03/10/2017 17:13

Kaspersky Lab, ha creato un pop-up shop in cui i dati personali o meglio, i Data Dollar, sono l'unica moneta utilizzabile. L'obiettivo è dimostrare che i dati hanno un valore economico che può essere utilizzato per gli acquisti nei negozi del futuro.

Roma, 3 ottobre 2017 - Il Data Dollar Store è stato creato e allestito da Kaspersky Lab in Old Street a Londra, nel cuore della capitale della tecnologia. I clienti si sono messi in coda molto presto per aggiudicarsi le stampe esclusive del noto street artist Ben Eine, ma sono rimasti molto sorpresi di fronte al modo con cui avrebbero dovuto pagare le opere d'arte, veniva in effetti chiesto a loro di rinunciare alle proprie fotografie personali o ai video e utilizzarli come metodo di pagamento per gli acquisti. Dopo la sorpresa iniziale hanno però acconsentito favorendo l'aumento della valuta Data Dollar. Il Data Dollar Store, è stato ideato per far crescere negli utenti la consapevolezza del valore effettivo dei dati personali e attirare altri player di mercato ad unirsi a questa attività utilizzando il simbolo del Data Dollar. Per l'occasione è stato realizzato un video.

I dati trattati

Dati personali: qualsiasi informazione che identifichi o renda identificabile, direttamente o indirettamente, una persona fisica. Informazioni che possono essere relative alle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

Particolarmente importanti sono:

- ✓ i **dati che permettono l'identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i **dati che permettono l'identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

- ✓ i **dati rientranti in particolari categorie**: si tratta dei dati c.d. "sensibili" cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il RE ha incluso nella nozione anche i **dati genetici,** i **dati biometrici** e quelli relativi all'**orientamento sessuale** - dati relativi alla salute;

- ✓ i **dati relativi a condanne penali e reati**: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il RE ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie, **altri dati personali** hanno assunto un ruolo significativo, come **quelli relativi alle comunicazioni elettroniche** (via Internet o telefono) e **quelli che consentono la geolocalizzazione**, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

I principi APPLICABILI al trattamento

a) **LICEITA', CORRETTEZZA E TRASPARENZA**

a) **LIMITAZIONE DELLA FINALITA'**

b) **ADEGUATEZZA, PERTINENZA, LIMITATEZZA (MINIMIZAZIONE DEL DATO)**

c) **ESATTEZZA**

d) **LIMITAZIONE DELLA CONSERVAZIONE**

e) **INTEGRITA' E RISERVATEZZA**

f) **RESPONSABILIZZAZIONE**

Il significato dei principi applicabili al trattamento dei dati

I dati devono essere:

a) trattati in modo, lecito, corretto e trasparente

b) raccolti per finalità determinate, esplicite, legittime

c) adeguati, pertinenti, non eccedenti

d) esatti e se necessario aggiornati

e) conservati in una forma che consenta l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati raccolti

f) trattati in maniera da garantire un'adeguata sicurezza mediante misure tecniche ed organizzative adeguate

Il consenso al trattamento del dato

E’ stato introdotto un articolo *ad hoc* per le condizioni per il consenso (art. 7)

Il consenso rientra tra le condizioni di liceità del trattamento, elencate dall’art. 6 del GDPR, e rappresenta il **principale diritto di controllo**, in capo all’interessato, per autorizzare il trattamento e per revocarlo – una volta accettato – in ogni momento senza ottenere pregiudizio.

Il consenso è: “***qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell’interessato con la quale lo stesso manifesta il proprio assenso mediante dichiarazione o azione positiva inequivocabile che i dati personali che lo riguardano siano oggetto di trattamento”.***

Il consenso al trattamento del dato

Il consenso deve essere quindi:

- informato
- specifico
- libero
- inequivocabile

Il consenso deve essere preceduto da una valida informativa.

Il Gruppo dei Garanti europei, infatti, chiarisce che solo fornendo agli interessati le giuste e chiare informazioni sul trattamento, sarà possibile per l'interessato capire quello che sta accettando e decidere consapevolmente se fornire il consenso o meno.
Il consenso, perché sia informato, deve basarsi su alcune informazioni necessarie, ritenute i requisiti minimi per ottenere un valido consenso.

Il consenso al trattamento del dato

- linguaggio chiaro, semplice, comprensibile
- richiesta di consenso chiaramente distinguibile
- revocabilità del consenso in qualsiasi momento
- specificazioni per il consenso dei minori per i servizi della società dell'informazione

onere della prova del consenso in capo al titolare

Liceità del trattamento: il consenso

Il trattamento dei dati è lecito solo se è consentito dalla legge. Il consenso è quindi uno dei tanti modi per legittimare/autorizzare, ma anche revocare, le attività di trattamento che vengono svolte.

Consenso: qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale lo stesso **manifesta il proprio assenso**, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Il RE, come il vecchio codice privacy, vieta di trattare alcune categorie di dati, ma prevede in alcuni casi, il trattamento come legittimo strumento.

Trattamento è legittimo per motivi di interesse pubblico proporzionato alla finalità perseguita, ma è anche legittimo per poter eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: con il nuovo RE NON è più necessario chiedere il consenso al trattamento cosiddetto consenso base.

Rimane però necessario per trattare dati come quelli relativi alla ricerca, sperimentazioni, DSE, dati genetici, ecc. Non deve essere necessariamente documentato per iscritto, ma non è comunque ammesso il consenso tacito o presunto.

Informativa: trasparenza del trattamento

Il Titolare del trattamento deve **adottare le misure appropriate** per fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma **(1) concisa, (2) trasparente, (3) intelligibile e (4) facilmente accessibile**, utilizzando un linguaggio semplice e chiaro.

L'interessato deve essere messo nella condizione di poter comprendere sempre come saranno trattati i suoi dati personali.
Le informazioni devono essere fornite per iscritto o con altri mezzi, anche elettronici.

Per informativa si intende **quell'insieme di informazioni che il titolare del trattamento è tenuto a fornire ad ogni interessato**, verbalmente o per iscritto.

Informativa: trasparenza del trattamento

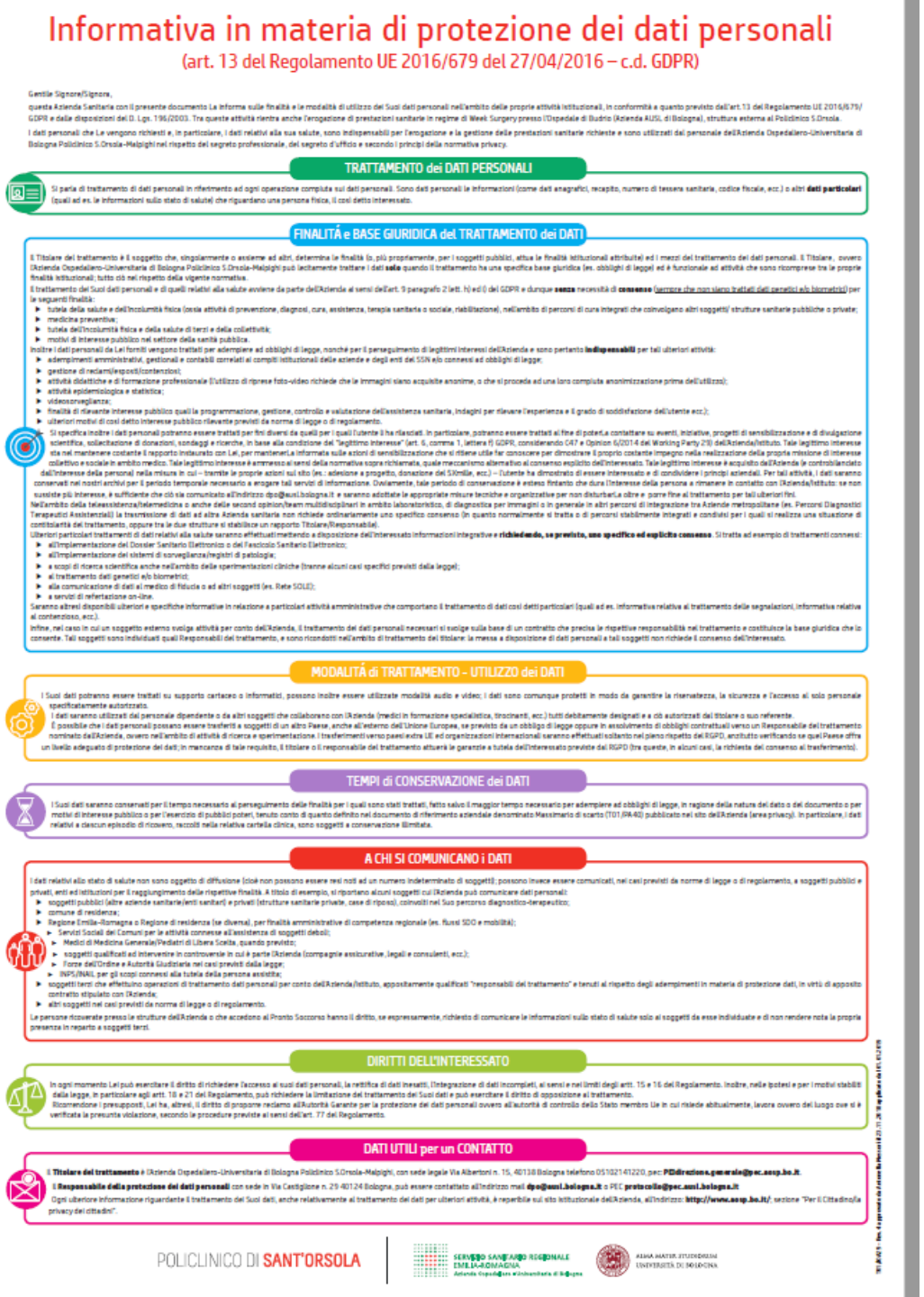
L’informativa è uno strumento che rimane, ma che deve essere rimodernato in quanto necessario per **garantire un trattamento corretto e trasparente.**

QUANDO: da fornire prima dell’esecuzione del trattamento (raccolta) del dato

COSA: deve contenere tutti i campi indicati da RE (es. **gli scopi e le modalità** del trattamento; se l’interessato **è obbligato o no** a fornire i dati; quali sono **le conseguenze** se i dati non vengono forniti; a chi possono essere **comunicati o diffusi** i dati; quali sono **i diritti riconosciuti** all’interessato; chi sono **il titolare** e l’eventuale responsabile del trattamento; d**ove sono raggiungibili** questi soggetti, ecc.)

COME: per iscritto, con un linguaggio chiaro e semplice, quindi comprensibile e sintetica - concisa, idonea alle diverse tipologie di interessati (anche usando icone ed immagini)

Esempio di una informativa



Informativa in materia di protezione dei dati personali

(art. 13 del Regolamento UE 2016/679 del 27/04/2016 – c.d. GDPR)

Gentile Signore/Signora,
questa Azienda Sanitaria con il presente documento La informa sulle finalità e le modalità di utilizzo dei Suoi dati personali nell'ambito delle proprie attività istituzionali, in conformità a quanto previsto dall'art.13 del Regolamento UE 2016/679/GDPR e dalle disposizioni del D. Lgs. 196/2003. Tra queste attività rientra anche l'erogazione di prestazioni sanitarie in regime di Week Surgery presso l'Ospedale di Budrio (Azienda AUSL di Bologna), struttura esterna al Policlinico S.Orsola.
I dati personali che Le vengono richiesti e, in particolare, i dati relativi alla sua salute, sono indispensabili per l'erogazione e la gestione delle prestazioni sanitarie richieste e sono utilizzati dal personale dell'Azienda Ospedaliero-Universitaria di Bologna Policlinico S.Orsola-Malpighi nel rispetto del segreto professionale, del segreto d'ufficio e secondo i principi della normativa privacy.

TRATTAMENTO dei DATI PERSONALI

Si parla di trattamento di dati personali in riferimento ad ogni operazione compiuta sui dati personali. Sono dati personali le informazioni (come dati anagrafici, recapito, numero di tessera sanitaria, codice fiscale, ecc.) o altri **dati particolari** (quali ad es. le informazioni sullo stato di salute) che riguardano una persona fisica, il cosi detto interessato.

FINALITÀ e BASE GIURIDICA del TRATTAMENTO dei DATI

Il Titolare del trattamento è il soggetto che, singolarmente o assieme ad altri, determina le finalità (o, più propriamente, per i soggetti pubblici, attua le finalità istituzionali attribuite) ed i mezzi del trattamento dei dati personali. Il Titolare, ovvero l'Azienda Ospedaliero-Universitaria di Bologna Policlinico S.Orsola-Malpighi può lecitamente trattare i dati **solo** quando il trattamento ha una specifica base giuridica (es. obblighi di legge) ed è funzionale ad attività che sono ricomprese tra le proprie finalità istituzionali, tutto ciò nel rispetto della vigente normativa.
Il trattamento dei Suoi dati personali e di quelli relativi alla salute avviene da parte dell'Azienda ai sensi dell'Art. 9 paragrafo 2 lett. h) ed i) del GDPR e dunque **senza** necessità di **consenso** (tenendo che non siano trattati dati genetici e/o biometrici) per le seguenti finalità:

- tutela della salute e dell'incolumità fisica (ossia attività di prevenzione, diagnosi, cura, assistenza, terapia sanitaria o sociale, riabilitazione), nell'ambito di percorsi di cura integrati che coinvolgono altri soggetti/ strutture sanitarie pubbliche o private;
- medicina preventiva;
- tutela dell'incolumità fisica e della salute di terzi e della collettività;
- motivi di interesse pubblico nel settore della sanità pubblica.

Inoltre i dati personali da Lei forniti vengono trattati per adempiere ad obblighi di legge, nonché per il perseguimento di legittimi interessi dell'Azienda e sono pertanto **indispensabili** per tali ulteriori attività:

- adempimenti amministrativi, gestionali e contabili correlati ai compiti istituzionali delle aziende e degli enti del SSN e/o connessi ad obblighi di legge;
- gestione di reclami/esposti/contenziosi;
- attività didattiche e di formazione professionale (l'utilizzo di riprese foto-video richiede che le immagini siano acquisite anonime, o che si proceda ad una loro compiuta anonimizzazione prima dell'utilizzo);
- attività epidemiologica e statistica;
- videosorveglianza;
- finalità di rilevante interesse pubblico quali la programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, indagini per rilevare l'esperienza e il grado di soddisfazione dell'utente ecc.);
- ulteriori motivi di così detto interesse pubblico rilevante previsti da norma di legge o di regolamento.

Si specifica inoltre i dati personali potranno essere trattati per fini diversi da quelli per i quali l'utente li ha rilasciati. In particolare, potranno essere trattati al fine di poterLa contattare su eventi, iniziative, progetti di sensibilizzazione e di divulgazione scientifica, sollecitazione di donazioni, sondaggi e ricerche, in base alla condizione del "legittimo interesse" (art. 6, comma 1, lettera f) GDPR, considerando C47 e Opinion 6/2014 del Working Party 29) dell'Azienda/Istituto. Tale legittimo interesse sta nel mantenere costante il rapporto instaurato con Lei, per mantenerLa informata sulle azioni di sensibilizzazione che si ritiene utile far conoscere per dimostrare il proprio costante impegno nella realizzazione della propria missione di interesse collettivo e sociale in ambito medico. Tale legittimo interesse è ammesso ai sensi della normativa sopra richiamata, quale meccanismo alternativo al consenso esplicito dell'interessato. Tale legittimo interesse è acquisito dall'Azienda (e controllando dall'interesse della persona) nella misura in cui – tramite le proprie azioni sul sito (es.: adesione a progetto, donazione del 5Xmille, ecc.) – l'utente ha dimostrato di essere interessato e di condividere i principi aziendali. Per tali attività, i dati saranno conservati nei nostri archivi per il periodo temporale necessario a erogare tali servizi di informazione. Ovviamente, tale periodo di conservazione è esteso fintanto che dura l'interesse della persona a rimanere in contatto con l'Azienda/Istituto: se non sussiste più interesse, è sufficiente che ciò sia comunicato all'indirizzo dpo@ausl.bologna.it e saranno adottate le appropriate misure tecniche e organizzative per non disturbarLa oltre e porre fine al trattamento per tali ulteriori fini.
Nell'ambito della teleassistenza/telemedicina o anche delle second opinion/team multidisciplinari in ambito laboratoristico, di diagnostica per immagini o in generale in altri percorsi di integrazione tra Aziende metropolitane (es. Percorsi Diagnostici Terapeutici Assistenziali) la trasmissione di dati ad altra Azienda sanitaria non richiede ordinariamente uno specifico consenso (in quanto normalmente si tratta o di percorsi stabilmente integrati e condivisi per i quali si realizza una situazione di contitolarità del trattamento, oppure tra le due strutture si stabilisce un rapporto Titolare/Responsabile).
Ulteriori particolari trattamenti di dati relativi alla salute saranno effettuati mettendo a disposizione dell'interessato informazioni integrative e **richiedendo, se previsto, uno specifico ed esplicito consenso**. Si tratta ad esempio di trattamenti connessi:

- all'implementazione del Dossier Sanitario Elettronico o del Fascicolo Sanitario Elettronico;
- all'implementazione dei sistemi di sorveglianza/registri di patologia;
- a scopi di ricerca scientifica anche nell'ambito delle sperimentazioni cliniche (tranne alcuni casi specifici previsti dalla legge);
- al trattamento dati genetici e/o biometrici;
- alla comunicazione di dati al medico di fiducia o ad altri soggetti (es. Rete SOLE);
- a servizi di refertazione on-line.

Saranno altresì disponibili ulteriori e specifiche informative in relazione a particolari attività amministrative che comportano il trattamento di dati così detti particolari (quali ad es. informativa relativa al trattamento delle segnalazioni, informativa relativa al contenzioso, ecc.).
Infine, nel caso in cui un soggetto esterno svolga attività per conto dell'Azienda, il trattamento dei dati personali necessari si svolge sulla base di un contratto che precisa le rispettive responsabilità nel trattamento e costituisce la base giuridica che lo consente. Tali soggetti sono individuati quali Responsabili del trattamento, e sono ricondotti nell'ambito di trattamento del titolare: la messa a disposizione di dati personali a tali soggetti non richiede il consenso dell'interessato.

MODALITÀ di TRATTAMENTO – UTILIZZO dei DATI

I Suoi dati potranno essere trattati su supporto cartaceo o informatici, possono inoltre essere utilizzate modalità audio e video; i dati sono comunque protetti in modo da garantire la riservatezza, la sicurezza e l'accesso al solo personale specificatamente autorizzato.
I dati saranno utilizzati dal personale dipendente o da altri soggetti che collaborano con l'Azienda (medici in formazione specialistica, tirocinanti, ecc.) tutti debitamente designati e a ciò autorizzati dal titolare o suo referente.
È possibile che i dati personali possano essere trasferiti a soggetti di un altro Paese, anche all'esterno dell'Unione Europea, se previsto da un obbligo di legge oppure in assolvimento di obblighi contrattuali verso un Responsabile del trattamento nominato dall'Azienda, ovvero nell'ambito di attività di ricerca e sperimentazione. I trasferimenti verso paesi extra UE ed organizzazioni internazionali saranno effettuati soltanto nel pieno rispetto del RGPD, accertato verificando se quel Paese offra un livello adeguato di protezione dei dati; in mancanza di tale requisito, il titolare o il responsabile del trattamento attuerà le garanzie a tutela dell'interessato previste dal RGPD (tra queste, in alcuni casi, la richiesta del consenso al trasferimento).

TEMPI di CONSERVAZIONE dei DATI

I Suoi dati saranno conservati per il tempo necessario al perseguimento delle finalità per i quali sono stati trattati, fatto salvo il maggior tempo necessario per adempiere ad obblighi di legge, in ragione della natura del dato o del documento o per motivi di interesse pubblico o per l'esercizio di pubblici poteri, tenuto conto di quanto definito nel documento di riferimento aziendale denominato Massimario di scarto (T01.PA40) pubblicato nel sito dell'Azienda (area privacy). In particolare, i dati relativi a ciascun episodio di ricovero, raccolti nella relativa cartella clinica, sono soggetti a conservazione illimitata.

A CHI SI COMUNICANO i DATI

I dati relativi allo stato di salute non sono oggetto di diffusione (cioè non possono essere resi noti ad un numero indeterminato di soggetti); possono invece essere comunicati, nei casi previsti da norme di legge o di regolamento, a soggetti pubblici e privati, enti ed istituzioni per il raggiungimento delle rispettive finalità. A titolo di esempio, si riportano alcuni soggetti cui l'Azienda può comunicare dati personali:

- soggetti pubblici (altre aziende sanitarie/enti sanitari) e privati (strutture sanitarie private, case di riposo), coinvolti nel Suo percorso diagnostico-terapeutico;
- comune di residenza;
- Regione Emilia-Romagna o Regione di residenza (se diversa), per finalità amministrative di competenza regionale (es. flussi SDO e mobilità);
- Servizi Sociali dei Comuni per le attività connesse all'assistenza di soggetti deboli;
- Medici di Medicina Generale/Pediatri di Libera Scelta, quando previsto;
- soggetti qualificati ad intervenire in controversie in cui è parte l'Azienda (compagnie assicurative, legali e consulenti, ecc.);
- Forze dell'Ordine e Autorità Giudiziaria nei casi previsti dalla legge;
- INPS/INAIL per gli scopi connessi alla tutela della persona assistita;
- soggetti terzi che effettuino operazioni di trattamento dati personali per conto dell'Azienda/Istituto, appositamente qualificati "responsabili del trattamento" e tenuti al rispetto degli adempimenti in materia di protezione dati, in virtù di apposito contratto stipulato con l'Azienda;
- altri soggetti nei casi previsti da norma di legge o di regolamento.

Le persone ricoverate presso le strutture dell'Azienda o che accedono al Pronto Soccorso hanno il diritto, se espressamente richiesto di comunicare le informazioni sullo stato di salute solo ai soggetti da esse individuate e di non rendere nota la propria presenza in reparto a soggetti terzi.

DIRITTI DELL'INTERESSATO

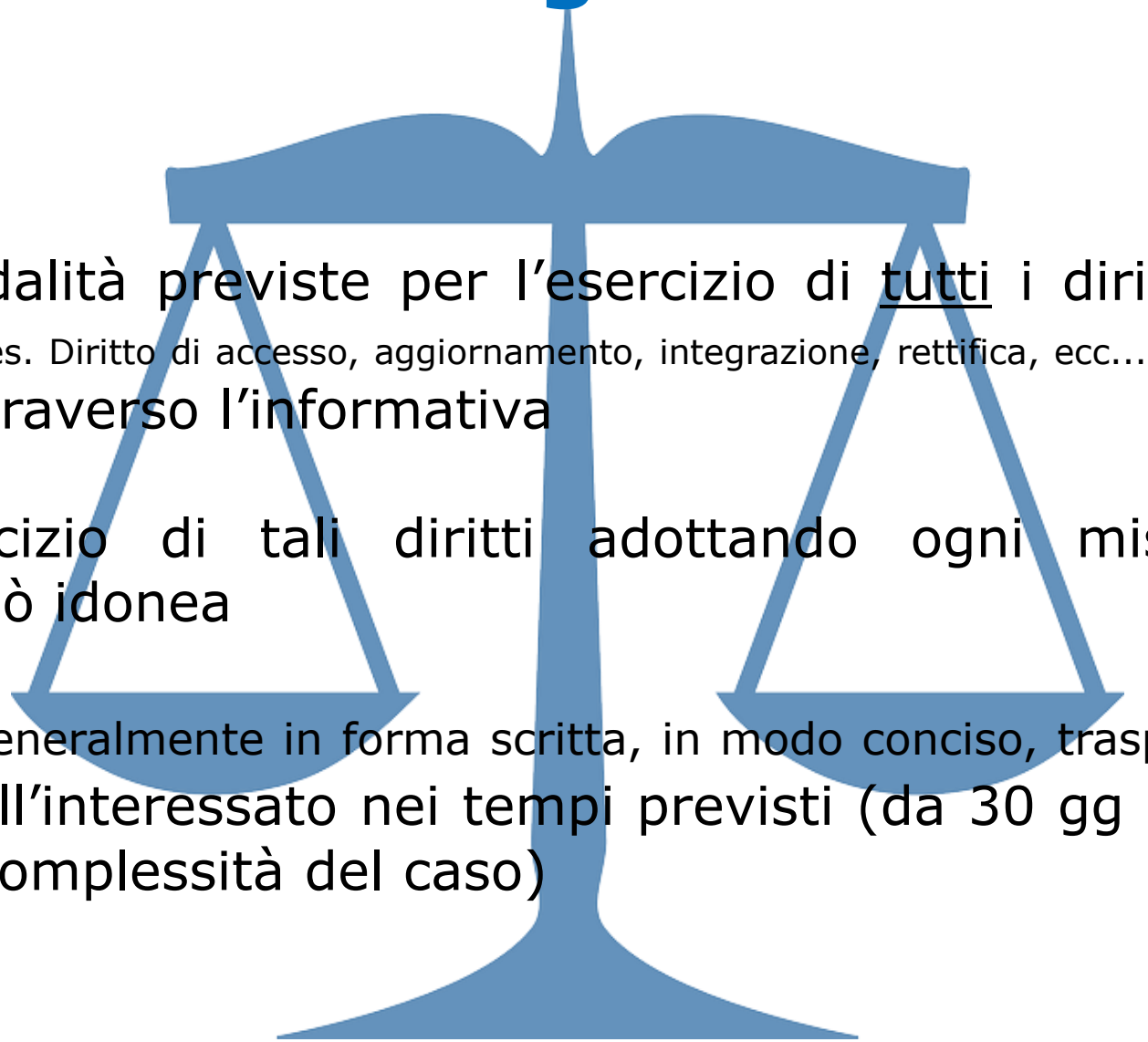
In ogni momento Lei può esercitare il diritto di richiedere l'accesso ai suoi dati personali, la rettifica di dati inesatti, l'integrazione di dati incompleti, ai sensi e nei limiti degli artt. 15 e 16 del Regolamento. Inoltre, nelle ipotesi e per i motivi stabiliti dalla legge, in particolare agli artt. 18 e 21 del Regolamento, può richiedere la limitazione del trattamento dei Suoi dati e può esercitare il diritto di opposizione al trattamento.
Ricordandone i presupposti, Lei ha, altresì, il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali ovvero all'autorità di controllo dello Stato membro Ue in cui risiede abitualmente, lavora ovvero del luogo ove si è verificata la presunta violazione, secondo le procedure previste ai sensi dell'art. 77 del Regolamento.

DATI UTILI per un CONTATTO

Il **Titolare del trattamento** è l'Azienda Ospedaliero-Universitaria di Bologna Policlinico S.Orsola-Malpighi, con sede legale Via Albertoni n. 15, 40138 Bologna telefono 0510214220, pec: **PEdirezione.generale@pec.aosp.bo.it**.
Il **Responsabile della protezione dei dati personali** con sede in Via Castiglione n. 29 40124 Bologna, può essere contattato all'indirizzo mail **dpo@ausl.bologna.it** o PEC **protocollo@pec.ausl.bologna.it**
Ogni ulteriore informazione riguardante il trattamento dei Suoi dati, anche relativamente al trattamento dei dati per ulteriori attività, è reperibile sul sito istituzionale dell'Azienda, all'indirizzo: **http://www.aosp.bo.it/**, sezione "Per il Cittadino/la privacy del cittadino".

POLICLINICO DI SANT'ORSOLA | SERVIZIO SANITARIO REGIONALE EMILIA-ROMAGNA | ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

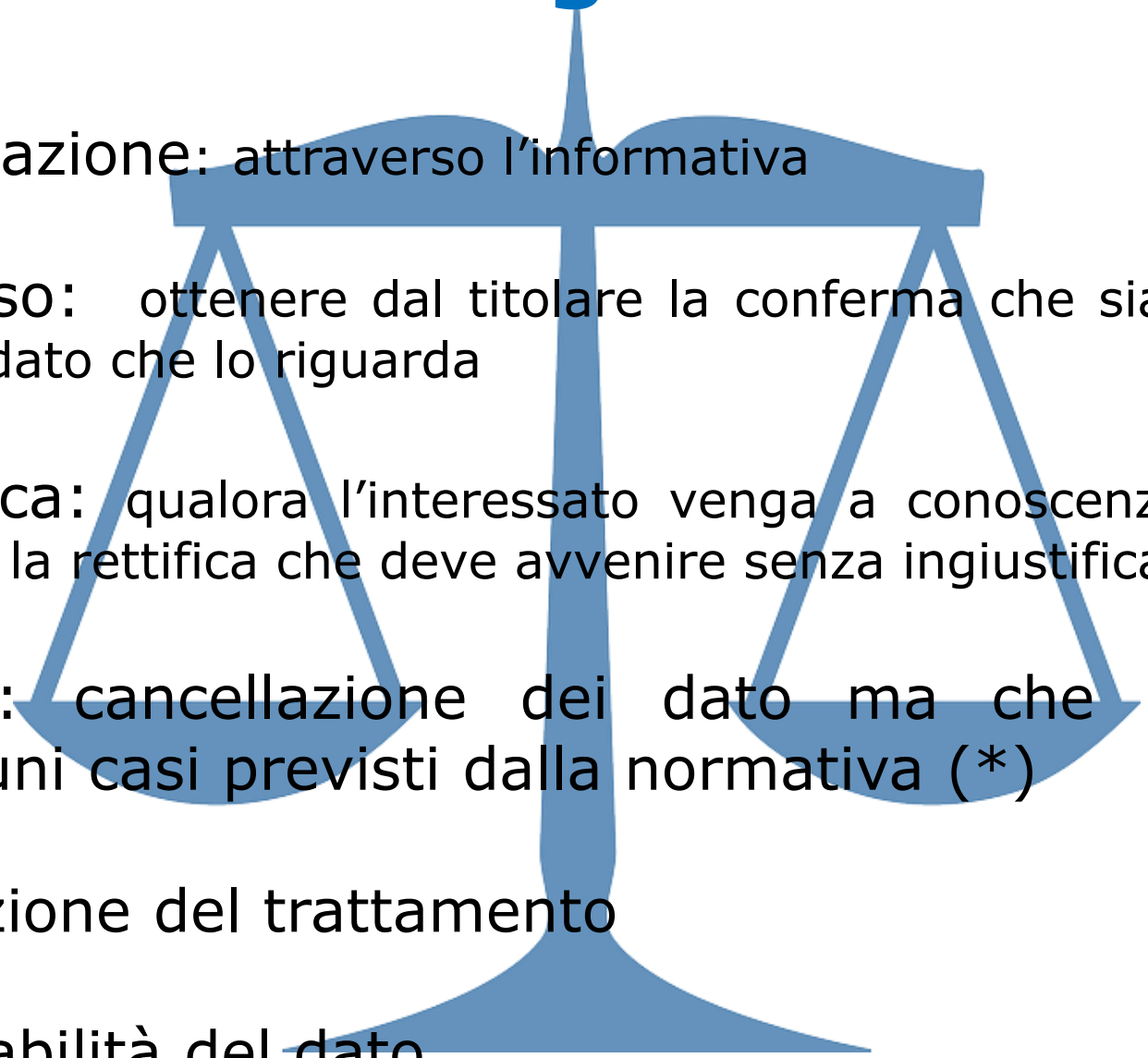
I diritti degli interessati



Il titolare deve:

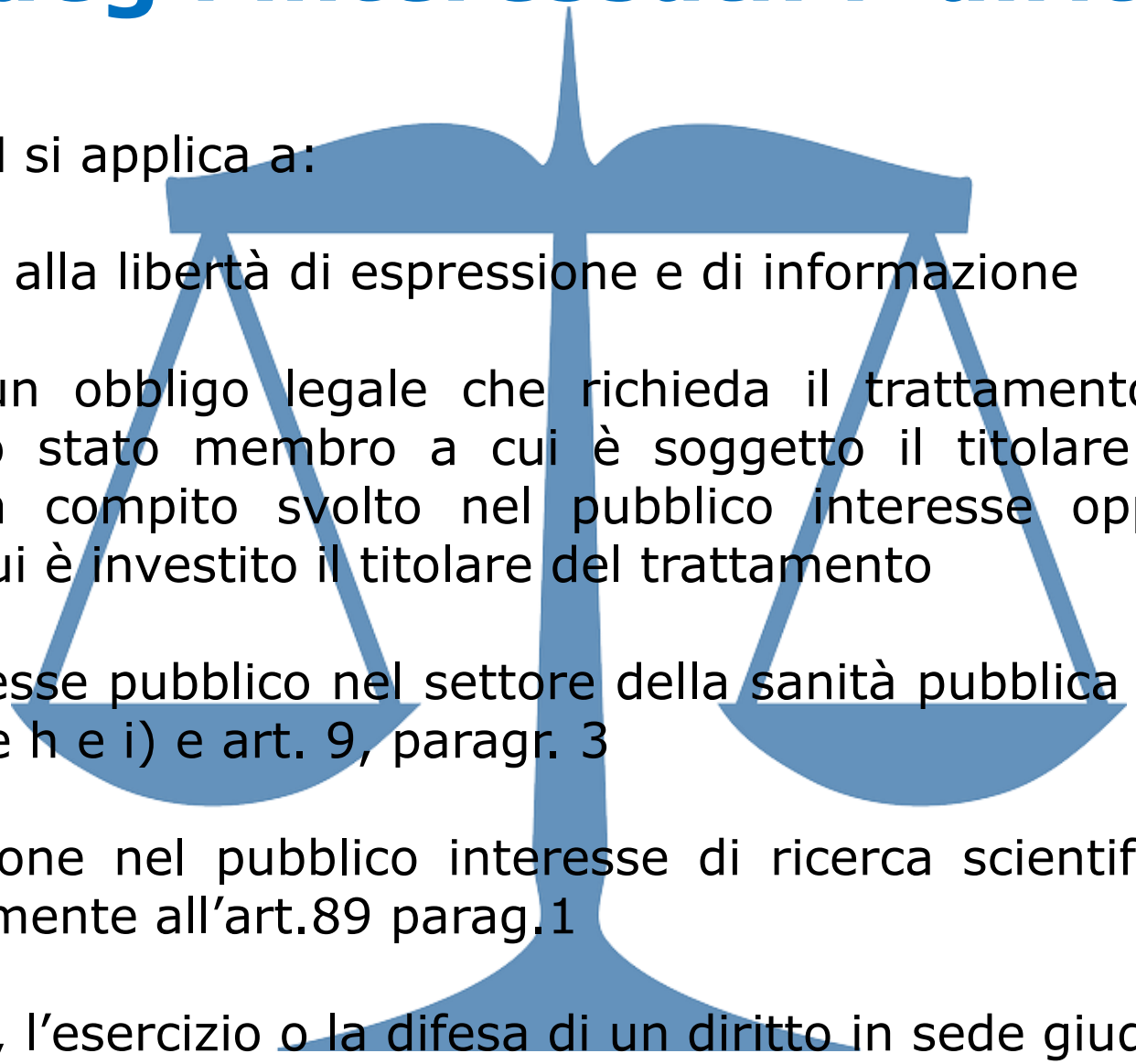
- ✓ rispettare le modalità previste per l'esercizio di tutti i diritti degli interessati stabilite dal RE (es. Diritto di accesso, aggiornamento, integrazione, rettifica, ecc....) quindi comunicati all'interessato attraverso l'informativa
- ✓ agevolare l'esercizio di tali diritti adottando ogni misura tecnica ed organizzativa a ciò idonea
- ✓ dare riscontro, generalmente in forma scritta, in modo conciso, trasparente, con linguaggio semplice e chiaro, all'interessato nei tempi previsti (da 30 gg estendibile a 90 gg a seconda della complessità del caso)

I diritti degli interessati



- ✓ Diritto di informazione: attraverso l'informativa
- ✓ Diritto di accesso: ottenere dal titolare la conferma che sia o meno in corso un trattamento di un dato che lo riguarda
- ✓ Diritto di rettifica: qualora l'interessato venga a conoscenza di inesattezze può chiedere al titolare la rettifica che deve avvenire senza ingiustificato ritardo
- ✓ Diritto all'oblio: cancellazione dei dato ma che NON può essere applicato in alcuni casi previsti dalla normativa (*)
- ✓ Diritto di limitazione del trattamento
- ✓ Diritto alla portabilità del dato

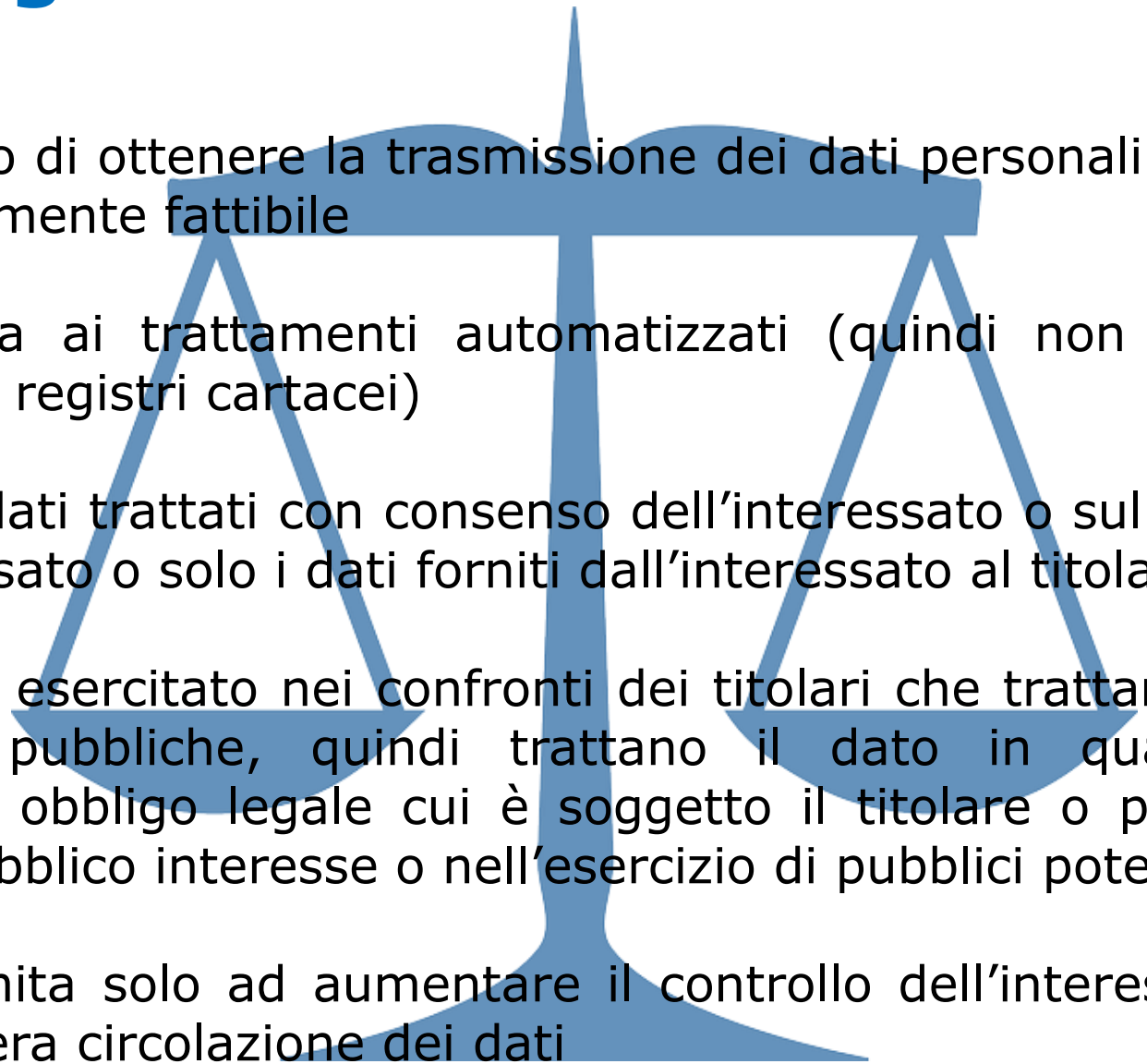
I diritti degli interessati: il diritto all'oblio



Il diritto all'oblio **NON** si applica a:

- esercizio del diritto alla libertà di espressione e di informazione
- adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'unione o dello stato membro a cui è soggetto il titolare del trattamento per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento
- per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'art. 9, paragr. 2, lettere h e i) e art. 9, paragr. 3
- a fini di archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici conformemente all'art.89 parag.1
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria

I diritti degli interessati: il diritto alla portabilità



L’interessato ha diritto di ottenere la trasmissione dei dati personali da un titolare «senza ostacoli» se è tecnicamente fattibile

Tale diritto si applica ai trattamenti automatizzati (quindi non alla documentazione contenuta in archivi o registri cartacei)

Sono portabili solo i dati trattati con consenso dell’interessato o sulla base di un contrato stipolato con l’interessato o solo i dati forniti dall’interessato al titolare

Non dovrebbe essere esercitato nei confronti dei titolari che trattano i dati nell’esercizio delle loro funzioni pubbliche, quindi trattano il dato in quanto necessario per l’adempimento di un obbligo legale cui è soggetto il titolare o per l’esecuzione di un compito svolto nel pubblico interesse o nell’esercizio di pubblici poteri

Tale diritto non si limita solo ad aumentare il controllo dell’interessato ai suoi dati ma favorisce anche la libera circolazione dei dati

Approccio basato sul RISCHIO e MISURE di ACCOUNTABILITY - 1

Il titolare tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto del contesto e delle finalità di trattamento come del rischio deve adottare le **misure tecniche ed organizzative ADEGUATE** a garantire un **livello di sicurezza ADEGUATO al rischio**. Spetta al titolare individuare specificatamente i rischi legati al trattamento dei dati e valutare quali misure di sicurezza tecniche, organizzative procedurali adottare. Questo è nello specifico l'espressione del concetto di accountability.

Approccio basato sul RISCHIO e MISURE di ACCOUNTABILITY - 2

Privacy by default and by design:

Al titolare è richiesta un'analisi dell'organizzazione aziendale e dei sistemi che coinvolgono i trattamenti dei dati personali e la protezione dei dati deve essere garantita fin dalla progettazione (by design) ed in maniera predefinita (by default).

E' la necessità di configurare il trattamento dei dati che viene svolto prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del RE e tutelare i diritti degli interessati.

L'articolo richiede al titolare una analisi preventiva ed un impegno applicativo che deve tradursi in attività specifiche e dimostrabili.

Es la pseudoanonimizzazione, ovvero l'attribuzione di un codice identificativo alla persona interessata, in luogo delle sue generalità, per impedirne luna diretta identificazione., oppure la criptazione dei dati particolari come quelli genetici, visualizzazione di dati come sesso o età ma non la generalità della persona.

Approccio basato sul RISCHIO e MISURE di ACCOUNTABILITY - 3

Registro dei trattamenti: il titolare deve censire i trattamenti svolti andando ad indicare una serie di elementi e predisporre obbligatoriamente un **registro** delle operazioni di trattamento i cui contenuti sono definiti dal RE (es. dati anagrafici del titolare, finalità del trattamento, categorie di interessati, tipologia dati trattati, categorie dei destinatari, trasferimento di dati personali, termini eventuali di cancellazione, descrizione delle di sicurezza tecnico-organizzative). Tale strumento fondamentale per il titolare ai fini di una eventuale ispezione del Garante, ha lo scopo di fornire un quadro aggiornato dei trattamenti in essere in una azienda, indispensabile per la valutazione e analisi dei rischi. Deve essere in forma scritta, anche elettronica e deve essere fornito su richiesta del Garante

Approccio basato sul RISCHIO e MISURE di ACCOUNTABILITY - 4

Compilato il registro il titolare deve valutare i RISCHI connessi alle attività svolte e agli impatti legati alla protezione dei dati.
Può basarsi ad esempio su:

RISCHI INTERNI: legati ai processi e attività di trattamento del dato
RISCHI ESTERNI: legati al fornitore
RISCHI TECNOLOGICI: legati alla sicurezza dell'infrastruttura
RISCHI DI GESTIONE: legati all'organizzazione interna

Alcuni esempi di possibili trattamenti ad alto rischio in sanità sono rappresentati da:
Gestione del Fascicolo Sanitario Elettronico
Utilizzo di dispositivi impiantabili
Gestione del Dossier Sanitario Elettronico

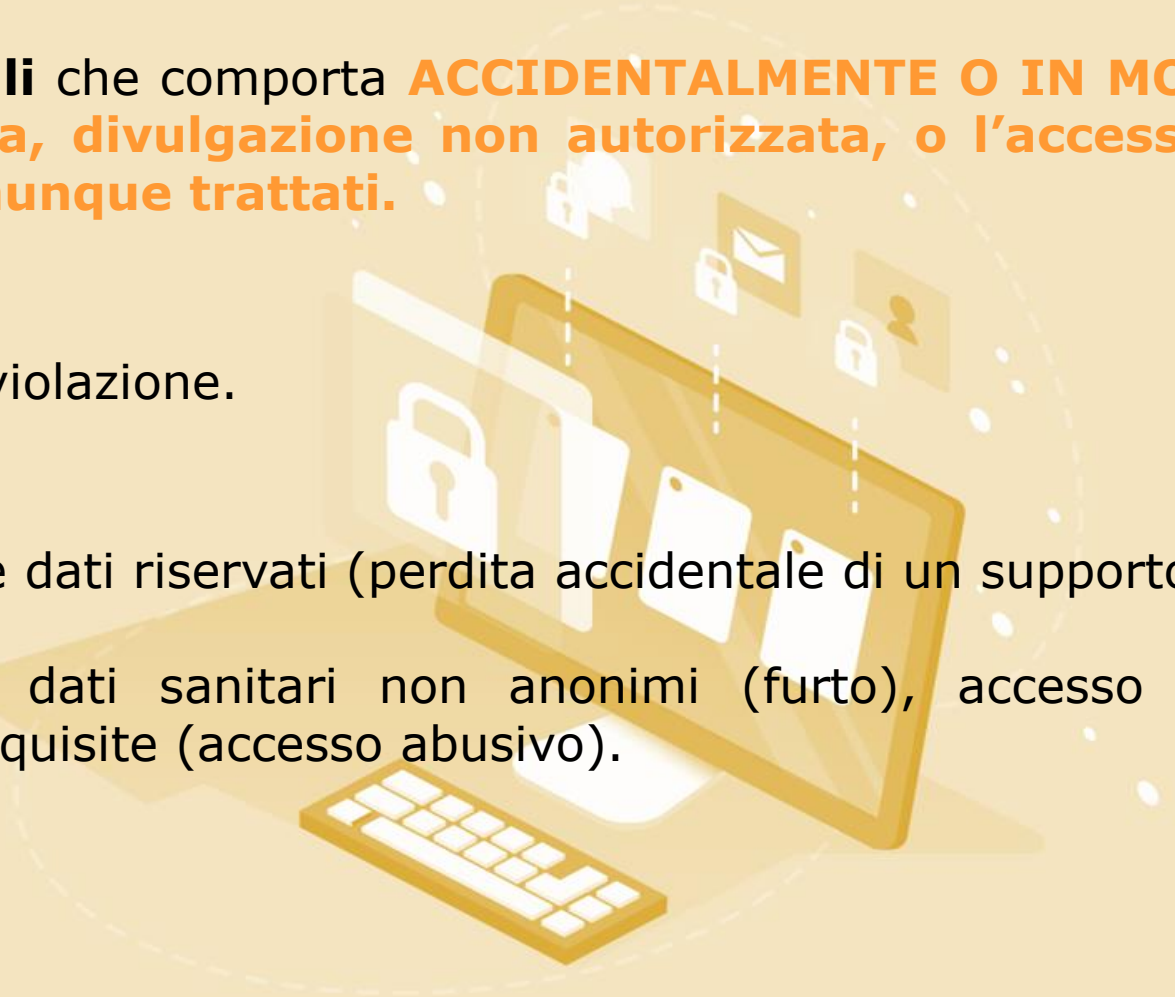
Approccio basato sul RISCHIO e MISURE di ACCOUNTABILITY -5

Misure di sicurezza: è un obbligo del titolare, dover garantire un livello di sicurezza **ADEGUATO** al rischio del trattamento con l'obiettivo di evitare la distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato, ecc…). Il RE cita es. la pseudoanonimizzazione (trattamento di dato che non permetta più l'attribuzione ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni siano conservate separatamente e soggette a misure intese a garantire che tali dati non siano attribuiti ad una persona fisica identificata o identificabile) , cifratura, misure per garantire la riservatezza, disponibilità, integrità, ecc.. Misure atte a garantire il tempestivo ripristino della disponibilità di dati, procedure per verificare e valutare regolarmente l'efficacia delle misure di sicurezza adottate.

Notifica di violazione di dati personali: il titolare deve notificare le violazioni di dati personali di cui venga a conoscenza **entro 72 ore** e "comunque senza ingiustificato ritardo", se ritenga probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. La notifica NON è obbligatoria essendo subordinata alla valutazione del rischio per gli interessati che spetta al titolare. Se la probabilità è elevata si dovrà informare anche l'interessato sempre "senza ingiustificato ritardo". Le violazioni vanno documentate anche se non notificate all'Autorità di controllo.

Approccio basato sul RISCHIO e MISURE di ACCOUNTABILITY - 6

Data breach – violazione dei dati personali che comporta **ACCIDENTALMENTE O IN MODO ILLECITO la distruzione, perdita, modifica, divulgazione non autorizzata, o l'accesso a dati personali trasmessi, conservati o comunque trattati.**



Va definito un percorso per la gestione di una violazione.

Alcuni esempi di data breach possono essere:

- smarrimento di una cartella clinica,
- smarrimento di una chiavetta USB contenete dati riservati (perdita accidentale di un supporto),
- scambio di referti,
- furto di un postatile aziendale contente dati sanitari non anonimi (furto), accesso non autorizzato e divulgazione di informazioni acquisite (accesso abusivo).

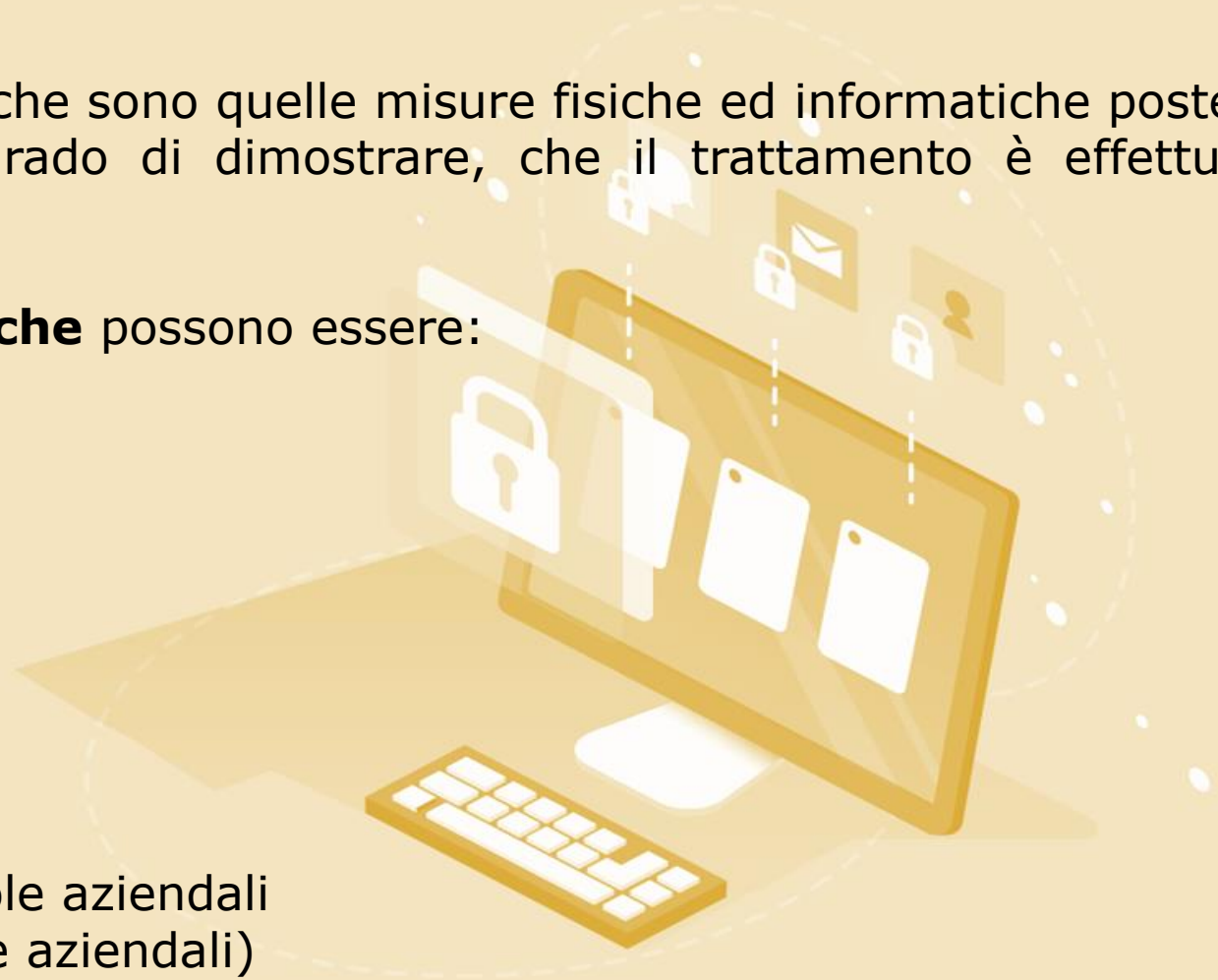
Approccio basato sul RISCHIO e MISURE di ACCOUNTABILITY - 6

Vanno inoltre identificate le misure tecniche che sono quelle misure fisiche ed informatiche poste in essere al fine di garantire ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al RE.

Alcuni esempi di **misure di sicurezza tecniche** possono essere:
protezione dei locali con allarmi,
accesso controllato ai locali,
smaltimento di rifiuti cartacei ed elettronici

Esempi di **misure organizzative**:
Formazione del personale
Verifiche interne

Esempi di **misure informatiche**:
Sicurezza delle reti (autenticazione) con regole aziendali
Sicurezza dei dispositivi personali (con regole aziendali)



Approccio basato sul RISCHIO e MISURE di ACCOUNTABILITY -7

Responsabile della protezione dei dati: anche la designazione del cosiddetto DPO (Data Protecion Officer) riflette l'approccio responsabilizzante che è proprio del RE.

La designazione è un obbligo, il RE tratteggia le caratteristiche soggettive ed oggettive di questa figura (es. indipendenza, autorevolezza, competenza).

I suoi compiti sono i seguenti:

- ✓ Informare e fornire consulenza al titolare, nonché ai dipendenti che eseguono attività di trattamento in merito agli obblighi derivanti dal RE
- ✓ Sorvegliare l'osservanza del RE
- ✓ Fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati personali
- ✓ Cooperare con l'Autorità di controllo
- ✓ Fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento dei dati

Sicurezza informatica di un dato

Il titolare deve definire le regole per l'accesso sicuro ai sistemi informatici e l'utilizzo delle risorse informatiche.

Ad esempio definire i criteri di accesso ad un sistema informativo (username e password), i criteri di gestione delle password, cifratura, pseudoanonimizzazione, vanno definiti obblighi generali di sicurezza al fine di garantire:

Riservatezza: protezione dati trasmessi o conservati per evitarne l'intercettazione o accesso a persone non autorizzate
Integrità: che i dati trasmessi ricevuti, conservati siano completi e inalterati
Disponibilità: i dati devono essere accessibili, e i servizi funzionare anche in caso di interruzioni dovute ad eventi eccezionali
Resilienza: intesa come obbligo di adottare misure volte a limitare l'impatto di un attacco a serie di informazioni o dati e risorse, evitando il perpetrarsi di ulteriori danni, che come capacità di reazione di un sistema a fronte di un evento che metta a rischio la sicurezza delle informazioni e dei dati trattati

Sicurezza informatica di un dato

Le misure di sicurezza che un titolate attraverso il servizio informatico può mettere in atto sono numerose, ad esempio:

- Organizzare momenti formativi
- Definire procedure scritte e aggiornandole periodicamente
- Limitare l'accesso agli utenti autorizzati
- Rivedere le autorizzazioni al fine di identificare e eliminare account non utilizzati,
- Predisporre un sistema di tracciabilità al fine di determinare l'origine di un data breach
- Prevenire gli attacchi di virus o accessi fraudolenti
- Predisporre meccanismi di blocco automatico della sessione in caso di inutilizzo della postazione
- Installare un firewall utilizzando un antivirus e software regolarmente aggiornati
- Limitare l'accesso internet
- Gestire le reti wi-fi
- Rafforzare le misure di sicurezza dei server
- Eseguire back up periodici
- Crittografare dati sensibili

Trasferimento di dati verso paesi terzi

Non possono esservi limitazioni né divieti alla libera circolazione dei dati personali nell'UE; pertanto non vi sono limiti per quanto riguarda i flussi di dati dall'Italia verso gli altri stati membri dell' UE. **E' vietato** il trasferimento di dati verso paesi non appartenenti alla UE. Il divieto può essere superato SOLO quando intervengono alcune garanzie specifiche:

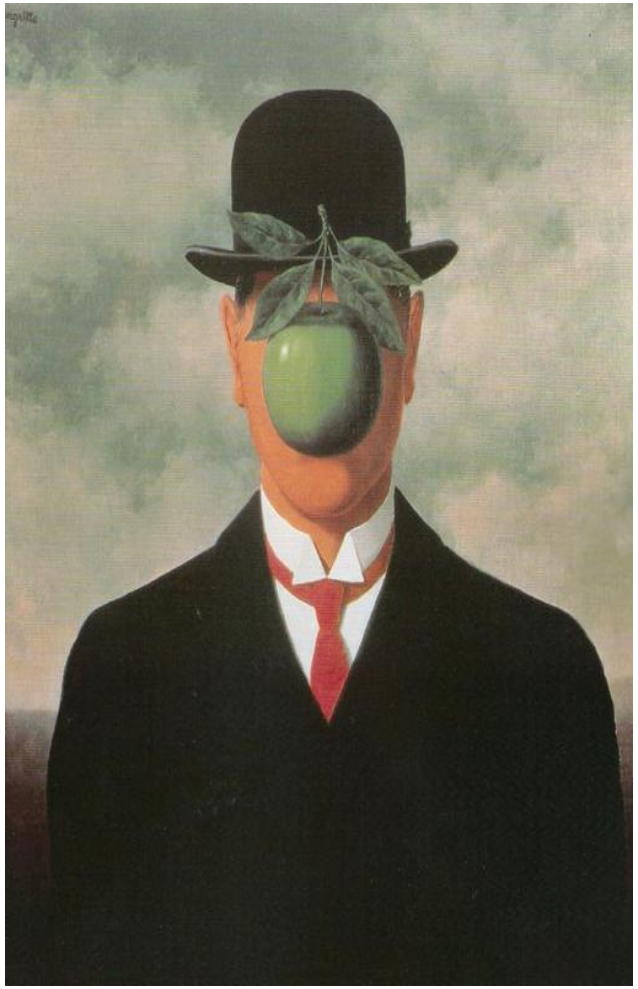
- ✓ **adeguatezza** del paese terzo riconosciuta tramite decisione della Commissione Europea;
- ✓ **garanzie adeguate** fornite dai titolari coinvolti nel trattamento (BCR, clausole contrattuali);
- ✓ in assenza di ogni precedente presupposto si utilizzano **deroghe** al divieto definite dal RE (art. 49).

Il titolare del trattamento dei dati ha quindi la **responsabilità** di garantire che i dati personali siano protetti e che i requisiti del RE siano rispettati che si traduce nell'**obbligo di garantire la protezione e la riservatezza** dei dati personali quando questi vengono trasferiti all'esterno della struttura.

L’autorità di controllo

E’ il **GARANTE per la protezione dei dati personali**
con sede a Roma

- ✓ un'**autorità amministrativa indipendente** dotata di **poteri di indagine, correttivi autorizzativi, consultivi, sanzionatori**
- ✓ un **organo collegiale** composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile
- ✓ deve **sorvegliare la corretta applicazione del Regolamento** al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con particolare riguardo al trattamento e agevolare la libera circolazione dei dati personali all’interno dell’unione



RECLAMO ALL'AUTORITA' GARANTE

L'**interessato**, può tutelare i propri dati personali inoltrando all'Autorità Garante un **reclamo** che deve contenere:

a) una indicazione per quanto possibile dettagliata dei fatti e circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste
b) gli estremi dei titolare o responsabile del trattamento
c) deve essere sottoscritto dall'interessato o su mandato dell'interessato da un ente terzo
d) dovranno essere allegati i documenti utili per provare quanto sostenuto e l'eventuale mandato indicando recapito per l'invio di comunicazioni anche tramite posta elettronica, fax o telefono.

L'Autorità garante:

a) esaminerà il reclamo,
b) eseguirà una istruttoria e se il reclamo NON risulterà manifestatamente infondato e sussistono i presupposti per adottare un provvedimento lo stesso potrà decidere mediante i poteri di cui dispone
c) emetterà un provvedimento che pubblicherà nella Gazzetta Ufficiale della Repubblica
d) dovrà adottare una decisione entro 9 mesi dal ricevimento del reclamo, sebbene entro 3 mesi deve avvisare l'interessato dello stato del procedimento; solo in via eccezionale qualora il reclamo sia particolarmente complesso, la decisione potrà essere emessa entro 12 mesi. Di tale dilazione dei tempi l'interessato deve esserne informato.

IL SISTEMA SANZIONATORIO

Il RE ha riformulato attività e poteri delle Autorità di controllo, tra cui quello di infliggere le sanzioni amministrative pecuniarie che devono essere **effettive, proporzionate e dissuasive** in relazione ad ogni singolo caso. L'ammontare delle stesse tiene conto di una serie di elementi come natura, gravità e durata della violazione, carattere colposo e doloso, le misure adottate dal titolare per attenuare il danno subito dall'interessato, il grado di responsabilità del titolare, precedenti violazioni pertinenti, ecc.

Le sanzioni si aggirano attorno a 10.000.000 € o per le imprese fino al 2% del fatturato mondiale totale annuo per es la violazione di redigere una informativa con un linguaggio adeguato es ad un minore, violazione di un provvedimento del Garante, mancata valutazione di impatto per le attività di ricerca, ecc. ma sono previste anche sanzioni che superano i 20.000.000 o per le imprese fino al 4% del fatturato in caso di violazione delle diffusione di dati genetici, biometrici ecc.

CONSEGUENZE LEGATE ALLA VIOLAZIONE DELLA NORMATIVA

Il Regolamento riconosce tre profili di responsabilità: civile, penale, amministrativa

CIVILE: chiunque abbia subito un danno materiale o immateriale causato da una violazione del presente regolamento ha diritto di ottener il risarcimento del danno dal Titolare o responsabile del trattamento.

A differenza della precedente normativa qui si fa riferimento al danneggiato e non a chi ha cagionato il danno, ma ciò che è più importante è che ora si individua chiaramente il soggetto che deve risarcire: il titolare o responsabile.

AMMINISTRATIVA:
E' l'autorità di controllo che deve provvedere affinché le sanzioni amministrative siano effettive, proporzionate e dissuasive. L'autorità prima di infliggere una sanzione deve considerare diversi criteri per stabilire il tipo di sanzione e il relativo importo.

PENALE: trattamento illecito di danni.
L'articolo 167 del codice è stato riformulato in modo da continuare a punire penalmente diverse condotte consistenti nell'arrecare nocumento all'interessato in violazione di alcune specifiche e limitate disposizioni normative come ad esempio alcuni requisiti sul trattamento di dati particolari e sul trasferimento interinazione di dati.

In pratica …

Per applicare quanto previsto dal nuovo Regolamento, occorre un **lavoro di squadra** all’interno delle strutture/aziende.

KEEP CALM AND ABITUATI AL GDPR