Data Protection e banche dati sanitarie tra diritti dei pazienti e interessi della ricerca

Francesca Preite, Avvocato Libero Professionista in Reggio Emilia

Silvia Salardi, Università degli Studi di Milano-Bicocca, Dipartimento di Giurisprudenza

Gruppo di studio sugli studi osservazionali della SISMEC e progetto ricerca finalizzata

24 novembre 2016

Il nuovo Regolamento Europeo 2016/679 sulla protezione dei dati. Agenda items:

- -Principi generali della protezione dei dati a livello europeo
- -Obiettivi del Regolamento
- -Di quali dati disciplina l'uso il regolamento?
- -Consenso informato e presudonomizzazione
- -Consenso per scopi di ricerca
- -Governance: obblighi e responsabilità dei data controller
- Sanzioni
- -Alcuni rilievi critici: deviazione dagli obiettivi di armonizzazione e possibile impatto sull'uso dei dati a scopo di ricerca; carenza dati genetici

I principi generali in materia di protezione dei dati a livello EU

Diritto alla privacy ha due principali significati:

-diritto alla riservatezza, ovvero di escludere gli altri dalla conoscenza di proprie vicende personali e familiari (Art. 7 della Carta dei diritti fondamentali dell'UE)

-diritto alla protezione dei dati personali inteso come diritto ad avere il controllo sui propri dati (Art. 8 della Carta dei diritti fondamentali dell'UE; Art. 16 TFUE)

Diritto all'informazione:

Art. 10 Convenzione sui Diritti dell'Uomo e la Biomedicina (Convenzione di Oviedo)
Art. 16 Protocollo addizionale relativo ai testo genetici
Art. 26 Protocollo addizionale relativo alla ricerca biomedica

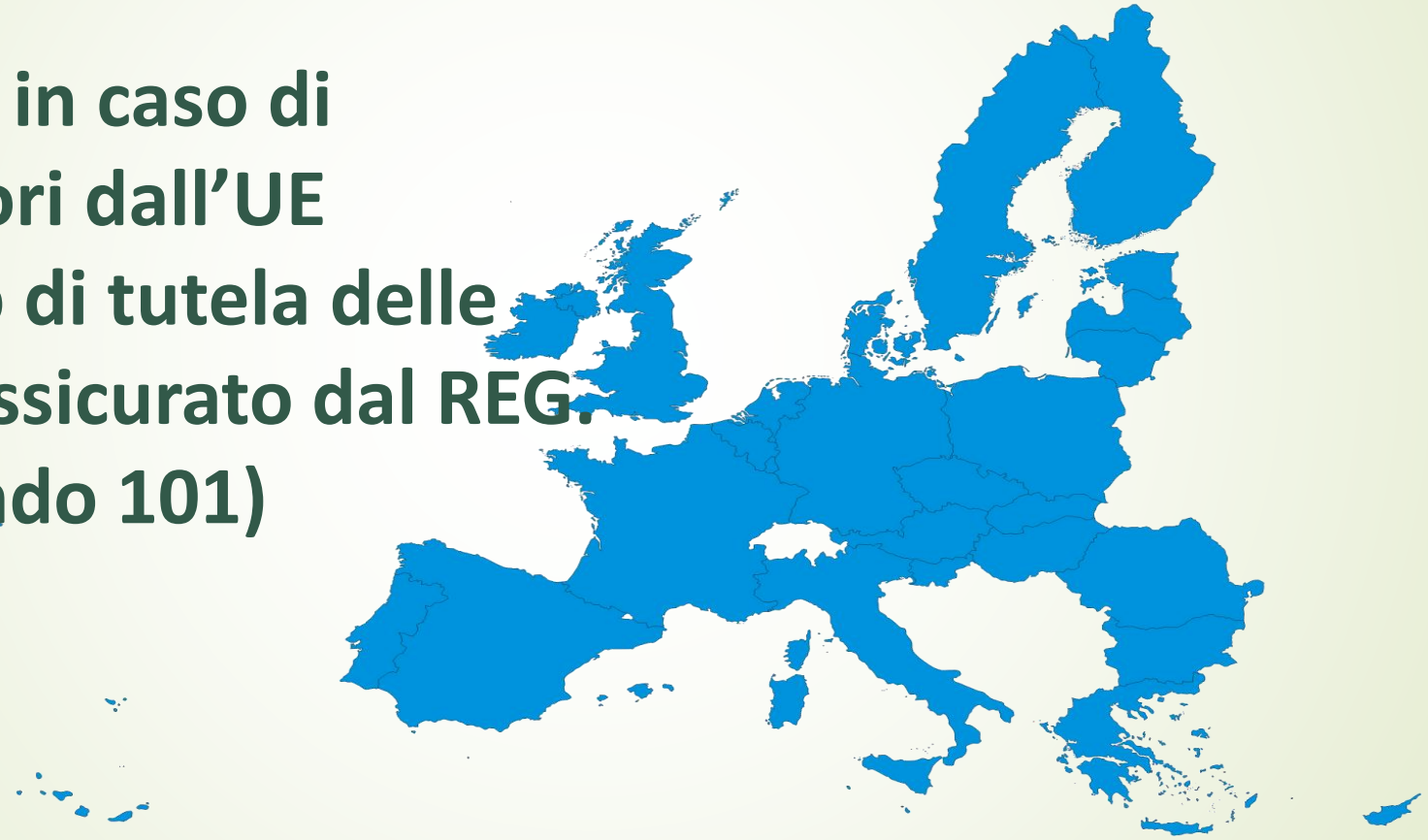
Regola generale prevista dalla Convenzione di Oviedo (Art. 2): L'interesse e il bene dell'essere umano devono prevalere sul solo interesse della scienza e della società

24 maggio 2016 > 24 maggio 2018

25 maggio 2018

Regolamento UE 2016/679	**IN VIGORE, NON APPLICABILE. SELF-EXECUTING**
Direttiva 1995/46	**IN VIGORE, DECADE il 24 maggio 2018**
Provvedimenti Autorità Garante	**NON DECADONO** fino a quando non verranno modificati, sostituiti, abrogati
Accordi internazionali su trasferimento dati	**NON DECADONO** fino a quando non verranno modificati, sostituiti, abrogati
Decisioni Commissione UE	**NON DECADONO** fino a quando non verranno modificate, sostituite, abrogate

REGOLAMENTO : in caso di trasferimento fuori dall'UE garantire il livello di tutela delle persone fisiche assicurato dal REG. in UE (considerando 101)



Obiettivi generali del Regolamento

-Garantire un livello coerente ed elevato di tutela delle persone fisiche

-Rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione

TUTTAVIA: gli Stati membri rimangono liberi di mantenere o introdurre norme nazionali al fine di precisare e specificare le norme del Regolamento

Di quali dati disciplina l'uso il Regolamento? Ambito di applicabilità

-I dati personali delle persone fisiche identificate o identificabili e la loro libera circolazione (Art. 4)

-Dati trattati interamente o parzialmente in modo automatizzato e trattamento non automatizzato di dati personali contenuti in archivio o destinati a figurarvi

-I dati pseudonimizzati sono dati codificati: le informazioni personali non possono essere attribuite ad un determinato soggetto, se non tramite l'utilizzo di informazioni aggiuntive

-Non si applica al trattamento dei dati personali delle persone decedute (considerando 27)

-Non si applica ai dati anonimi

Consenso informato, pseudonomizzazione e consenso per scopi di ricerca: in generale

- Il consenso informato è vincolo giuridico non solo per il trattamento dei dati personali, ma altresì per manifestare la volontà di partecipare ad uno studio.
- Pertanto, al paziente cui è richiesta la partecipazione ad uno studio è richiesta la firma di due distinti moduli di consenso, atti a garantire due diversi diritti: diritto all'autodeterminazione per la partecipazione ad uno studio e diritto alla privacy.
- Vi è stata un'apertura sia nel Reg. 679/2016 sia nel Reg. 536/2014 (Art. 28) relativo ai clinical trials verso un consenso più flessibile e non più 'narrow' o 'specific' in considerazione dei possibili mutamenti negli scopi della ricerca.

Consenso informato del paziente: prospettive in materia di ricerca clinica

- Non necessità del consenso per il trattamento dei dati dei pazienti deceduti (Reg. 679/2016)
- Al momento della sottoscrizione del consenso alla partecipazione alla ricerca si può chiedere di acconsentire all'uso dei dati al di fuori del protocollo specifico a fini esclusivamente di ricerca, con garanzia di poter revocare il consenso in qualsiasi momento (Reg. 536/2014)
- Possibilità al momento della raccolta dei dati per finalità di cura di esprimere un consenso a taluni settori della ricerca scientifica (Reg. 679/2016)
- TUTTAVIA: nonostante queste aperture il consenso è sempre un atto positivo inequivocabile, **MAI** un silenzio assenso

Consenso informato: prospettive in materia di ricerca clinica

- **TRATTAMENTO PER FINALITÀ COMPATIBILI:** Possibilità di usare il consenso dell'interessato per finalità diverse da quelle per cui i dati sono stati inizialmente raccolti, previa valutazione di compatibilità tra finalità iniziali e successive. L'uso a scopo di ricerca dovrebbe essere considerato sempre compatibile (considerando 50)
- **TRATTAMENTO SENZA CONSENSO**: Possibilità di derogare a norme sul consenso quando queste rendano impossibile o pregiudichino gravemente il conseguimento delle finalità di ricerca (Art. 89, 2 Reg. 679/2016) ossia:

  Impossibile comunicare l'informativa

  L'informativa implica risorse sproporzionate

  L'informativa rischia di pregiudicare gravemente gli obiettivi di ricerca scientifica

Garante per la Protezione dei Dati Personali

Autorizzazione generale al trattamento dei dati personali
per scopi di ricerca scientifica

Autorizza il trattamento senza consenso per scopi di ricerca:

- **4. Impossibilità di informare gli interessati.**
- L'autorizzazione riguarda il trattamento dei dati degli interessati da includere nella ricerca che non è possibile contattare al fine di fornire l'informativa - a causa della sussistenza di una delle seguenti ragioni, considerate del tutto particolari o eccezionali, documentate nel progetto di ricerca:
- 1. Motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione. Rientrano in questa categoria le ricerche per le quali l'informativa sul trattamento dei dati da rendere agli interessati comporterebbe la rivelazione di notizie concernenti la conduzione dello studio la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi (possono rientrare in questa ipotesi, ad esempio, gli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso per il quale non esista un trattamento).
- 2. Motivi di impossibilità organizzativa riconducibili alla circostanza che la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile contattare per informarli, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati; ciò avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti (ad esempio, nei casi in cui lo studio riguarda interessati con patologie ad elevata incidenza di mortalità o in fase terminale della malattia o in età avanzata e in gravi condizioni di salute).
- Con riferimento a tali motivi di impossibilità organizzativa, è autorizzato il trattamento dei dati di coloro i quali, all'esito di ogni ragionevole sforzo compiuto per contattarli, anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente, risultino essere al momento dell'arruolamento nello studio:
- - deceduti o
- - non contattabili.
- Resta fermo l'obbligo di raccogliere il consenso al trattamento dei dati degli interessati inclusi nella ricerca in tutti i casi in cui, nel corso dello studio, sia possibile rendere loro un'adeguata informativa e, in particolare, laddove questi si rivolgano al centro di cura, anche per visite di controllo.

PIÙ NEL DETTAGLIO DEL REGOLAMENTO

Responsabilità del titolare

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento **mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di *dimostrare*, che il trattamento è effettuato conformemente al presente regolamento**. Dette misure sono riesaminate e aggiornate qualora necessario.

Responsabile della protezione dei dati

Figura indipendente nominata dal titolare e dal responsabile del trattamento. Svolge le seguenti funzioni: informare e consigliare il Titolare o il Responsabile in merito agli obblighi del Regolamento, verificarne l'applicazione e l'attuazione, fornire pareri, fungere da punto di contattato sia con gli interessati che con il Garante.

Registro dei trattamenti

Contenente i dati del/dei titolare/i e degli eventuali responsabili, le finalità del trattamento, una descrizione delle categorie di interessati e dei dati personali, i destinatari, gli eventuali trasferimenti verso Paesi terzi ed una descrizione generale delle misure di sicurezza. Tali documenti devono essere messi a disposizione del Garante e manutenuti sia dal titolare che dagli eventuali responsabili. I registri di cui sono tenuti in forma scritta.

Protezione sin dalla progettazione

Le misure a protezione di dati devono essere adottate già al momento della progettazione di un prodotto o software.
Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire in ogni caso che siano trattati solo i dati necessari per ogni specifica finalità.

Responsabilità solidale di titolare e responsabile

Il Titolare e il Responsabile del trattamento sono responsabili in solido nei confronti dell'interessato, per un eventuale danno causato dal trattamento.

Responsabilità dei contitolari

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità.

Violazione di dati

Nel caso si verifichino violazioni di dati personali, il Titolare ne deve dare comunicazione all'Autorità di Controllo e, nei casi più gravi, anche agli interessati (attualmente ciò avviene solo per violazione di dati biometrici).

Eliminazione dell'obbligo di notifica

Viene eliminato l'obbligo generale di notificare all'autorità di controllo per il trattamento di dati personali, da sostituire con meccanismi e procedure efficaci che si concentrino piuttosto su quei trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche

Valutazione d'impatto

Sostituisce la notificazione. È la valutazione preliminare degli impatti a cui andrebbe incontro un processo qualora dovessero essere violate le misure di protezione dei dati. Necessita di alcune attività come la mappatura dei dati e dei trattamenti, la pianificazione degli interventi tecnologici e organizzativi di protezione dei dati con una valutazione complessiva di riduzione dello stato di rischio

Certificazioni

Richiesta volta ad ottenere il riconoscimento della conformità dei processi di trattamento dei dati al Regolamento.

Diritto all'oblio

Diritto di ottenere la cancellazione dei dati che lo riguardano purché non sussistano motivi legittimi per conservarli. Vi sono deroghe per i trattamenti in materia di ricerca (considerando 65, articolo 89, 2).

Diritto alla portabilità dei dati

Possibilità per l'interessato di ricevere i propri dati personali in un formato strutturato, leggibile da dispositivo automatico e di uso comune. Introduce, inoltre, il diritto di ottenere, salvo impedimenti tecnici, la trasmissione diretta dei dati da un Titolare all'altro di verifica.

RESPONSABILE DELLE PROTEZIONE DEI DATI

E' OBBLIGATORIO IN TRE CASI

1) autorità pubblica o organismo pubblico
2) controllo regolare e sistematico degli interessati su larga scala
3) trattamento, su larga scala, di categorie particolari di dati (tra cui dati sanitari)

- è una figura di vigilanza, **interna o esterna**
- un gruppo di imprese può nominare un unico DPO
- è designato in funzione delle qualità professionali
- coinvolto in tutte le questioni
- non deve ricevere istruzioni e non dev'essere in conflitto d'interessi e deve godere di autonomia e indipendenza

AUTORITÀ DI CONTROLLO

- AUTORITÀ PUBBLICA INDIPENDENTE ISTITUITA DA UNO STATO MEMBRO E RESPONSABILE DELL'APPLICAZIONE DEL REGOLAMENTO E A TAL FINE COLLABORA CON LE AUTORITÀ DI CONTROLLO DI ALTRI STATI E CON LA COMMISSIONE. (GARANTE PER LA PROTEZIONE DEI DATI)

VALUTAZIONE D'IMPATTO: CHI, QUANDO, PERCHÈ….

- **CHI LA ESEGUE?:** IL TITOLARE DEL TRATTAMENTO E IL RESPONSABILE DEL TRATTAMENTO
- **QUANDO?:** QUANDO IL TRATTAMENTO DEI DATI PUÒ PRESENTARE UN RISCHIO PER I DIRITTI E LE LIBERTÀ DELL'INTERESSATO
- **A COSA SERVE?:** A DETERMINARE L'ORIGINE , LA NATURA, LA PARTICOLARITÀ E LA GRAVITÀ DEL RISCHIO
- **A COSA CONDUCE L'ESITO DELLA VALUTAZIONE?:** A DETERMINARE LE MISURE DA ADOTTARE PER DIMOSTRARE CHE IL TRATTAMENTO È CONFORME AL REGOLAMENTO UE
- **COSA SUCCEDE SE EMERGE RISCHIO ELEVATO DI VIOLAZIONE?:** SE IL RISCHIO NON È ATTENUABILE CON MISURE OPPORTUNE IN RELAZIONE A TECNOLOGIE DISPONIBILI E COSTI DI ATTUAZIONE, BISOGNA CONSULTARE L'AUTORITÀ DI CONTROLLO

VALUTAZIONE D'IMPATTO…

QUANDO E' OBBLIGATORIA

1. USO DI NUOVE TECNOLOGIE CON RISCHIO PER INTERESSATI
2. PROFILAZIONE
3. CATEGORIE PARTICOLARI DI DATI SU LARGA SCALA (tra cui dati sanitari)
4. SORVEGLIANZA SU LARGA SCALA

VALUTAZIONE D'IMPATTO…

CONTENUTI

a) **descrizione** sistematica dei **trattamenti** previsti e delle finalità del trattamento,
b) **valutazione della necessità e proporzionalità** dei trattamenti in relazione alle finalità;
c) **valutazione dei rischi** per i diritti e le libertà degli interessati
d) **misure previste per affrontare i rischi**

VALUTAZIONE D'IMPATTO

AUTORITA' DI CONTROLLO

provvederà alla tenuta di un

ELENCO PUBBLICO

elenco delle tipologie di trattamenti per le quali

è o non è richiesta

una valutazione d'impatto sulla protezione dei dati

Sicurezza del trattamento

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche

titolare e responsabile

mettono in atto

misure tecniche e organizzative adeguate

per garantire un livello di sicurezza adeguato al rischio

*che comprendono, **tra le altre**, se del caso >*

- **Pseudonimizzazione**
- **Cifratura**
- **Capacità di**

1) assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
2) ripristinare ***tempestivamente*** la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

- **Procedura**

per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Pseudonimizzazione

- Principio della minimizzazione dei dati, ovvero i dati personali sono adeguati, pertinenti e limitati a quanto necessario per le finalità per cui sono trattati. Tale principio include:
  - La pseudonimizzazione: se le finalità possono essere eseguite in tal modo. TUTTAVIA, se è possibile trattamento che non rende più identificabile l'interessato, va utilizzato questo metodo. (Art. 89, 1 Reg. 679/2016)
- Se i dati sono resi sufficientemente anonimi, il Reg. non si applica

Quali prescrizioni sulla pseudonimizzazione nel REG EU?

- I dati personali sottoposti a pseudonimizzazione che potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni sono informazioni su una persona fisica identificabile:

- L'identificabilità comprende tutti I mezzi di cui ci si può avvalere per identificare la persona. Tra questi mezzi vanno considerati anche i costi e il tempo necessario per l'identificazione tenuto conto delle tecnologie disponibili all'atto del trattamento e degli sviluppi tecnologici.
- La pseudonimizzazione non preclude l'impiego di altre misure di protezione dei dati se necessarie.
- Per potersi parlare di privacy by default e by design è opportuno che la pseudonimizzaaione dei dati avvenga il prima possibile.

Notifica della violazione di dati (Data Breach)

- Il titolare del trattamento notifica la violazione ***all'autorità di controllo*** competente […] senza ingiustificato ritardo e, ove possibile, ***entro 72 ore*** dal momento in cui ne è venuto a conoscenza, ***a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche***.
- Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Comunicazione di una violazione di dati

- Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento ***comunica la violazione all'interessato*** senza ingiustificato ritardo.
- La ***comunicazione*** all'interessato ***non è richiesta*** se il titolare:

a) ha ***messo in atto le misure tecniche e organizzative*** adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, ***quali la cifratura***;

b) ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati.

Sanzioni amministrative (Art. 83)

- Se TITOLARE E RESPONSABILE NON ADEMPIONO AGLI OBBLIGHI
  - **SINO A 10 MLN DI EURO**
  - **O 2% -4% DEL FATTURATO MONDIALE TOTALE ANNUO** dell'anno precedente

Sanzioni penali (art. 84)

- Gli **Stati membri stabiliscono le norme relative alle altre sanzioni** per le violazioni del presente regolamento in particolare per le violazioni non soggette sanzioni amministrative pecuniarie

Rilievi critici

Sarà solo il RGPD a disciplinare la materia? NO

Considerando n. 8 del RGPD

Ove il presente regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, ***gli Stati membri possono***, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, ***integrare elementi del presente regolamento nel proprio diritto nazionale***.

Resta margine di autonomia per gli Stati membri

Permangono **competenze locali** ad esempio**:**

-Trattamento dei dati di persone decedute

-Trattamento dei dati genetici e biometrici (senza ostacolare la libera circolazione dati)

-Compatibilità del trattamento successivo con quello iniziale

-Definizione di condizioni e garanzie per i trattamenti a fini di ricerca scientifica

-Elenco dei trattamenti soggetti a valutazione d’impatto

Alcuni rilievi critici

- Armonizzazione delle normative nazionali sarà un procedimento complesso visti i rinvii e le specificazioni richieste

- Positiva l'apertura ad un consenso informato iniziale che renda possibile l'uso dei dati per ricerche future. Tuttavia, bisogna evitare il rischio che venga interpretato come 'open consent' nella prassi, sottovalutando i rischi legati all'uso di un consenso ampio (cfr. Paradigmatico è il caso della tribù Havasupai contro l'Università dell'Arizona: Havasupai Tribe of Havasupai Reservation v. Arizona Bd. of Regents, 204 P.3d 1063)

SOURCE: REGULATION (EU) No 679/2016 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)