



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA



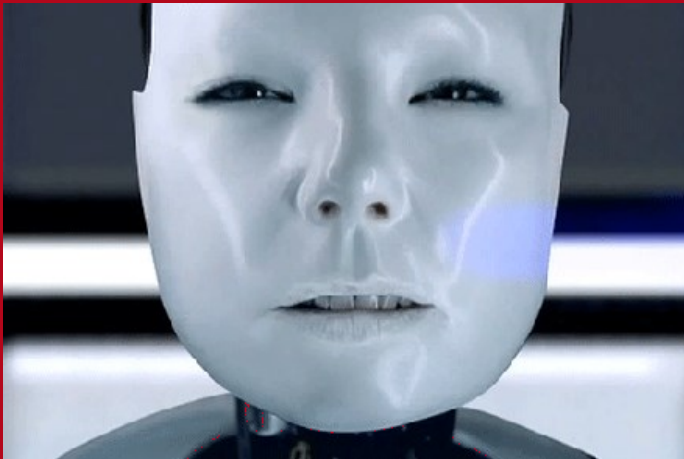
Dipartimento di Scienze Politiche,  
Giuridiche e Studi Internazionali

**Corso di Laurea in Informatica**  
***DIRITTO, INFORMATICA E SOCIETÀ' 2021-2022***

**Daniele Ruggiu**

**Padova 27, Maggio 2022**

# **Il Regolamento Generale Protezione Dati Personali**



## SOMMARIO

- ❖ Origine, struttura, scopi del Regolamento
- ❖ Soggetti e tipologie di dati
- ❖ Principi per il trattamento dati
- ❖ Diritti dell'interessato
- ❖ Obblighi del titolare del trattamento
- ❖ Protezione dati 'by design' e 'by default'
- ❖ Il 'Data Protection Officer'
- ❖ Il 'Data Protection Impact Assessment'
- ❖ Sanzioni



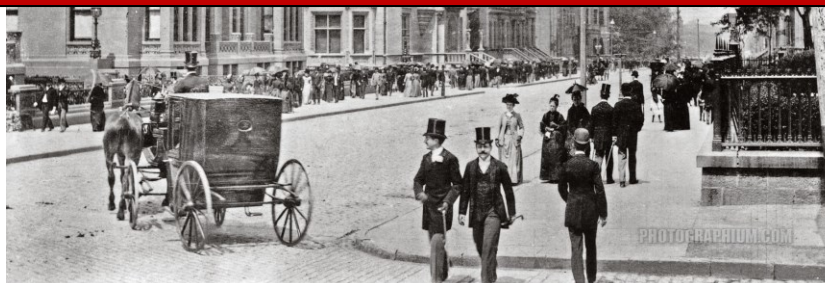


# Origine del concetto di privacy

- La privacy nasce nel 1890 in America con la nascita della fotografia come «right to be alone» in seguito ad un articolo di Samuel Warren e Louis Brandeis : diritto alla riservatezza, ognuno ha uno spazio riservato in cui fa accedere chi vuole

**è una sfera chiusa**

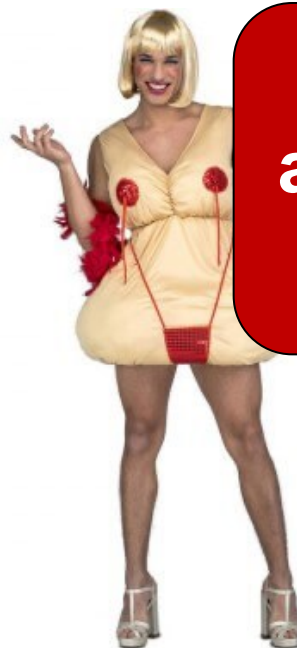
**proiezione dello spazio di  
autonomia del soggetto**





# Distinzione privacy e data protection

- Privacy : sfera sog
  - Protezione dei dati
- Es. foto del soggetto vestito da donna nella sua vita privata
- Es. le informazioni relative all'acquisto di un biglietto da Milano a Reggio Emilia
- Integrità dell'informazione (ogni soggetto dissemina informazioni che sfuggono al suo controllo da cui si può dedurre molto sulla sua vita)





- **Convenzione Europea per la protezione della democrazia e dei diritti umani** (art. 8 (Rispetto della vita privata e familiare)) del 1950
- **Convenzione sulla protezione delle persone rispetto al trattamento automatico dell'informatica personale** n. 108 del 1981

**diffusione dell'informatica  
di massa**

**Definizione di dato personale:  
ogni dato relativo ad una  
persona fisica identificata o  
identificabile**





# Nell'Unione europea

- **Trattato di Maastricht 1992** per l'integrazione del mercato unico

**Dati divengo fondamentali nel mercato**

- **Direttiva 46 del 1995** per avere una normativa quadro a livello europeo sulla protezione dei dati personali
  - Si fissano gli obiettivi
  - Gli Stati sono liberi di scegliere i mezzi per raggiungere gli obiettivi

**Necessità di una regolazione uniforme che vincoli gli Stati**

**Evitare che le differenze di regolazione all'interno della Ue e il *dumping***

**Regolamento immediatamente vincolante nell'Ue in modo uniforme**

**No libertà sui mezzi**



# Il Comitato europeo per la protezione dei dati

- Report del Comitato europeo per la protezione dei dati (Article 29 Data Protection Working Party)
  - gruppo di lavoro formato da esperti della direttiva sulla protezione dei dati in vigore del 1995, avevano lo scopo di occuparsi di questioni relative alla protezione della vita privata e dei dati personali.
  - Poi sostituito dall'**European Data Protection Board** (Comitato europeo per la protezione dei dati) un organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione.

**Guidelines 8/2020 on the targeting of  
social media users (14 aprile 2021)**





UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

## Gruppo di lavoro “Articolo 29”



#201968738

Dipartimento di Scienze Politiche,  
Giuridiche e Studi Internazionali

- **Regolamento Generale sulla Protezione dei Dati Personali, n. 2016/679**
- Un riferimento nella protezione della **privacy** e della **protezione dati** a livello mondiale
- Uno strumento ispirato alla protezione dei **diritti dei cittadini europei**

GDPR - Regolamento Europeo 2016/679



General  
Data  
Protection  
Regulation



Uno  
strumento  
rights-based

- Articolato su due concetti:
  - **privacy by design**
  - **privacy by default**



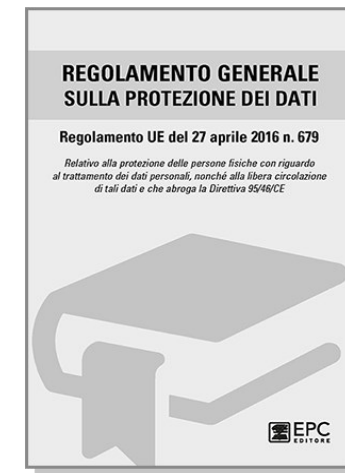
# Scopi del Regolamento

- Eliminare le differenze che impediscono la libera circolazione dati nel **mercato interno dell'Unione europea**
- Proteggere i **diritti fondamentali** dei cittadini europei



# La situazione in Italia

- Adottato il 26 aprile 2016
- Entrato in vigore il 25 maggio 2018
- C'era già il **Codice della privacy** e un sistema opt-in
  - I dati possono essere raccolti solo con il consenso
  - Il RGPD ha confermato il regime *opt-in*





# I soggetti del trattamento dei dati personali

## 1. Il titolare del trattamento

- La persona o l'istituzione che ha la responsabilità dell'intero trattamento

## 4. DPO – responsabile privacy

## 2. Il responsabile del trattamento

- Che esegue il trattamento per conto del titolare del trattamento

## 3. L'interessato

- La persona o l'impresa i cui dati sono trattati





UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

## LE FIGURE PREVISTE



di Scienze Politiche,  
Studi Internazionali



### **TITOLARE DEL TRATTAMENTO**

l'entità giuridica (impresa o  
ente) che decide motivo,  
finalità e quali dati raccogliere



### **RESPONSABILE DEL TRATTAMENTO**

colui che fisicamente elabora e gestisce i dati  
previsti dal titolare



### **RESPONSABILI DI SECONDO LIVELLO**

figure coinvolte dal Responsabile del Trattamento per svolgere  
alcuni compiti particolari.

- Dato
  - Qualunque informazione (personale o meno)
- Dato personale
  - Qualunque informazione che riguarda una persona fisica individuate individuabile
- Particolari categorie di dati
  - Dati in grado di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (Art. 9,1)
  - Dati personali relativi alle condanne penali e ai reati o a connessioni di sicurezza (Art. 10)



**Informazioni  
relative alla  
salute**

**Opinioni  
politiche e  
religiose**

**Preferenze  
sessuali**

**Informazioni su  
condanne penali e  
reati o connesse a  
misure di sicurezza**

• Non possono essere trattati a meno che l'interessato abbia prestato il consenso

• Trattamento senza il consenso

- Se è necessario per l'adempimento di un'obbligazione o il rispetto di un diritto del titolare del trattamento o dell'interessato
- Se è necessario per la protezione di un interesse vitale dell'interessato o di un'altra persona
- Se riguarda informazioni di pubblico dominio dell'interessato
- Il trattamento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria
- Se è necessario per ragioni di pubblico interesse nel campo della sanità
- Se è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici





UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

# Informazioni genetiche

Spogi

Dipartimento di Scienze Politiche,  
Giuridiche e Studi Internazionali

- Consenso
- E una autorizzazione ad hoc del Garante della privacy a carattere generale (Art. 9)





# I dati sono personali quando

- Non per la loro natura
- Non per la fonte da cui provengono
- Ma in quanto, anche se apparentemente irrilevanti, una volta integrati con altre informazioni sono in grado di identificare l'interessato (approccio funzionalistico)





- Normalmente è proibita
- Se il trattamento non richiede l'identificazione dell'interessato il responsabile del trattamento non è obbligato a conservare, acquisire trattare ulteriori informazioni per identificare l'interessato (Art. 11)



**informazioni  
già anonime**

# Principi per il trattamento dati (Art. 5)

1. Liceità, correttezza e trasparenza

**dati trattati in modo lecito,  
corretto e trasparente**

2. Principio della limitazione del trattamento

**per finalità determinate,  
esplicite e legittime**

3. Principio della minimizzazione dei dati

**adeguati, pertinenti e limitati a quanto  
necessario alle finalità del trattamento**

4. Principio dell'esattezza

**esatti e possibilmente  
aggiornati**

5. Principio della limitazione della conservazione

**conservati in modo da consentire l'identificazione per lo  
stretto necessario rispetto alle finalità del trattamento**

6. Principio dell'integrità e riservatezza

**trattati in modo sicuro**

- Quando si verifica una delle seguenti condizioni:
  - l'interessato abbia dato il **consenso**; o il trattamento è:
  - necessario per l'esecuzione di un **contratto** di cui l'interessato sia parte
  - necessario per l'adempimento di un **obbligo giuridico**
  - necessario per proteggere la **vita** dell'interessato o di un'altra persona
  - necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'esercizio di pubblici poteri
  - necessario per un **legittimo interesse** del titolare del trattamento o di terzi a condizione che non prevalgano sui diritti fondamentali dell'interessato



- Il Regolamento è costruito su un nucleo di diritti dell'interessato



- Diritto a prestare il **consenso** al trattamento dati (Art. 6) e al **ritiro** del consenso (Art. 7)







# Consenso al trattamento dei dati personali



- **esplicito** (art. 9,2 a)
  - manifestato prima che il trattamento abbia inizio
- **specifico** (art. 9,2 b)
  - relativo a finalità specifiche e determinate
- **informato** (Art. 13)
  - dato sulla base di informazioni chiare
- **documentabile** dal titolare del trattamento (Art. 7)

# Condizioni del consenso (Art. 7)

- Il titolare deve essere in grado di **dimostrare** che l'interessato abbia acconsentito
- Consenso prestato in modo da essere chiaramente **distinguibile da ogni altra materia** in una forma intelligibile e accessibile usando un linguaggio chiaro e semplice
- L'interessato ha il **diritto a ritirare** il consenso in qualsiasi momento



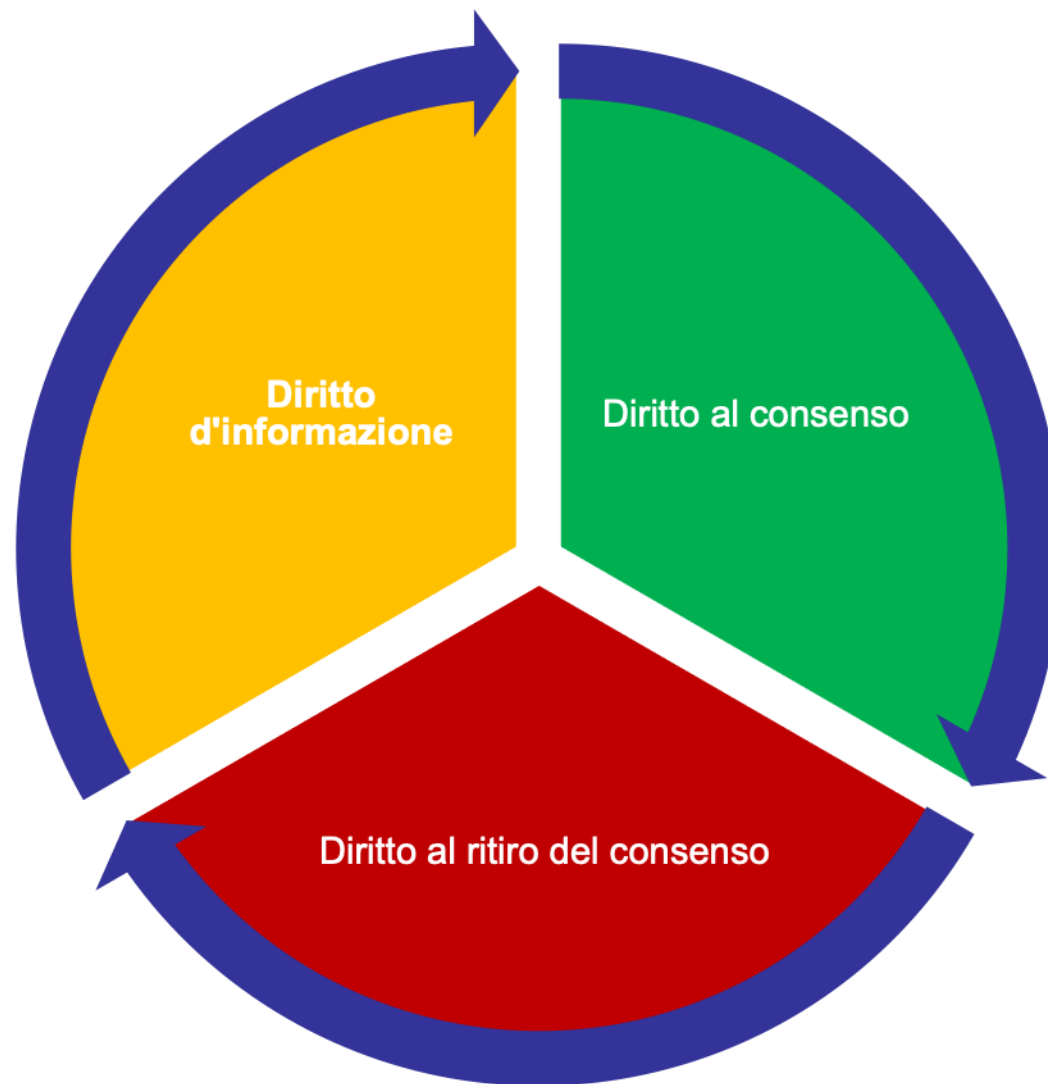


UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

# Struttura del Diritto al consenso

Spogi

Dipartimento di Scienze Politiche,  
Giuridiche e Studi Internazionali





UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

# Diritto all'informazione

## Linee guida del 2015 del Garante della privacy sui cookie di profilazione (Art. 13)

Spogi

Dipartimento di Scienze Politiche,  
Giuridiche e Studi Internazionali

- L'interessato deve essere informato
  - sul trattamento che lo riguarda e sui suoi diritti,
  - su chi è il titolare responsabile del trattamento,
  - su chi è il responsabile del trattamento e, eventualmente, su chi è il 'data protection officer',
  - sulle finalità del trattamento,
  - sulla durata del trattamento,
  - sull'eventuale esistenza di un trattamento automatizzato,
  - sulle misure tecniche adottate per la protezione dei dati (anonimizzazione, pseudonimizzazione, accesso ristretto, firewall, password etc.)

**in forma concisa, trasparente, intelligibile e  
facilmente accessibile, con un linguaggio  
semplice e chiaro**

- a ottenere la cancellazione dei dati da parte del titolare del trattamento
  - quando non sono più necessari per lo scopo per il quale sono stati raccolti
  - l'interessato ha ritirato il consenso
  - l'interessato si oppone al trattamento
  - i dati personali sono stati trattati in modo illecito
  - i dati personali devono essere cancellati per adempiere ad un obbligo giuridico

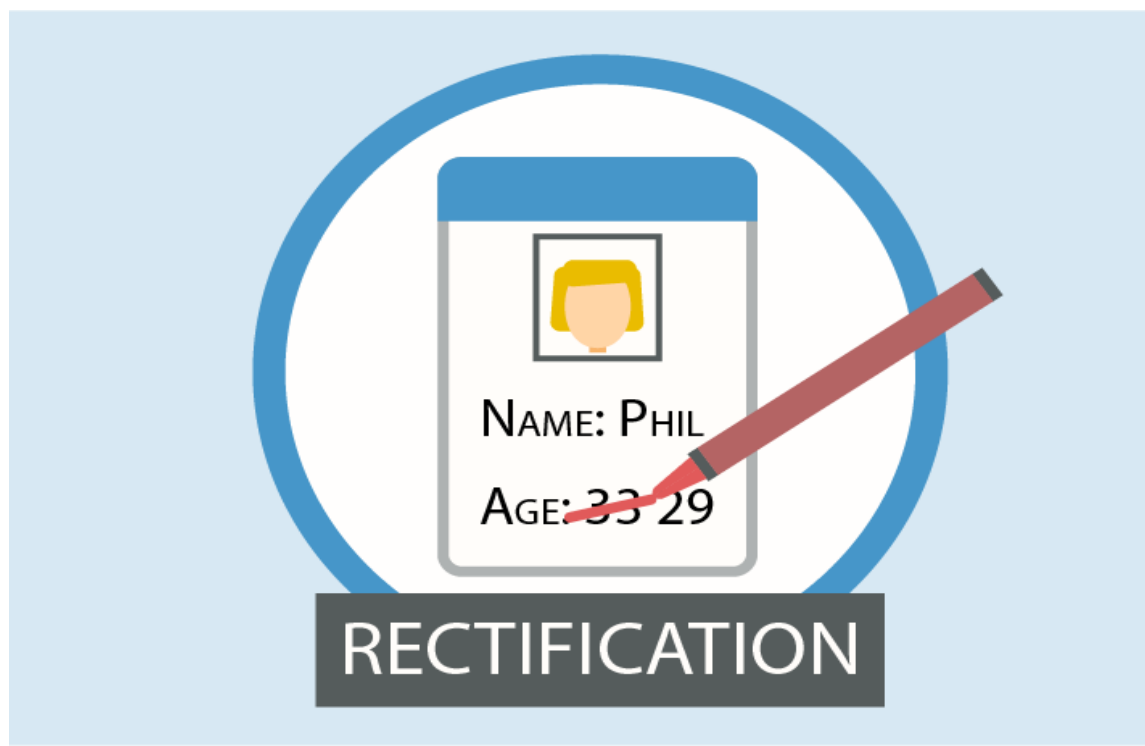




- diritto ad ottenere dal titolare
  - conferma sul fatto che esista un trattamento riguardante i propri dati personali
  - informazione sulle finalità del trattamento, sulle categorie di dati trattate, sulla durata del trattamento, sui destinatari a cui i dati saranno comunicati



- il diritto di richiedere dal titolare del trattamento la rettifica delle inesattezze rispetto ai dati personali trattati





# Diritto alla limitazione del trattamento (Art. 18)

- Il diritto a ottenere dal titolare del trattamento una limitazione del trattamento quando
  - si contesta l'esattezza dei dati personali
  - il trattamento è illecito e l'interessato si è opposto,
  - il titolare del trattamento non ha più bisogno dei dati per le finalità per le quali erano stati raccolti
  - l'interessato si è opposto al trattamento

- Il diritto di opporsi al trattamento dei propri dati personali (Art. 21)
- Il diritto a non essere sottoposti ad una decisione basata unicamente su un trattamento automatizzato (Intelligenza Artificiale) (Art. 22).





UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

# Diritto ad un ricorso giurisdizionale effettivo



Dipartimento di Scienze Politiche,  
Giuridiche e Studi Internazionali

- L'interessato ha diritto ad avere un concreto rimedio giurisdizionale per proteggere i propri diritti (Art. 79) e il diritto al risarcimento e responsabilità per i danni pecuniari e non che abbia sofferto (Art. 82).







- La violazione dei principi di base del trattamento, incluse le condizione del consenso (Artt. 5, 6, 7 e 9), rispetto ai diritti dell'interessato (Artt. 12, 13, 14, 15, 16, 17, 18, 21, e 22) è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente

€ 20M

4%  
OF ANNUAL  
GLOBAL  
REVENUE



# Obblighi del titolare del trattamento (Art. 25)

- mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento (principio di **responsabilità**)
  - misure tecniche per la protezione dei dati dell'interessato (anonimizzazione, pseudonimizzazione, restrizioni all'accesso, firewall, password etc.)
    - misure devono essere dimostrabili
- informare l'interessato
  - sul trattamento e i diritti dell'interessato
  - su chi è il titolare responsabile del trattamento
  - su chi è il responsabile del trattamento e il 'data protection officer'
  - sugli scopi del trattamento
  - sulla durata prevista del trattamento
  - sulle misure seguite nel trattamento
  - sulle misure per la protezione dei dati personali

# Protezione dati 'by design'

- Il titolare del trattamento mette in atto misure tecniche e organizzative per la protezione dei dati dell'interessato (sistemi di criptazione come anonimizzazione, pseudonimizzazione, restrizioni all'accesso, firewall, password etc.)





- Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita, solo i dati personali necessari** per ogni specifica finalità del trattamento. Tale obbligo vale per la **quantità** dei dati personali raccolti, la **portata del trattamento**, il **periodo** di conservazione e **l'accessibilità**.
- 'By default' i dati personali **non devono essere accessibili** ad un numero indefinito di persone senza che l'interessato abbia potuto intervenire





# Obblighi del responsabile del trattamento (Art. 28)

- tratta i dati per conto del titolare del trattamento
- mette in atto misure tecniche e organizzative adeguate
- garantisce che il trattamento rispetti i requisiti del Regolamento
- adotta le misure di sicurezza
- cancella o restituisce tutti i dati personali al titolare alla fine del trattamento
- fornisce al titolare le informazioni necessarie a dimostrare l'adempimento del Regolamento





# Data Protection Officer (Art. 27)

- Il soggetto incaricato dal titolare o dal responsabile del trattamento responsabile di fronte alle autorità di controllo e dell'interessato circa la protezione dei dati personali
- La nomina è necessaria (Art. 37) quando :
  - i) il trattamento è eseguito da una **pubblica autorità**
  - ii) il trattamento per sua natura, portata, finalità richiede il monitoraggio regolare e sistematico **su larga scala** degli interessati,
  - iii) il trattamento riguarda **particolari categorie di dati** (informazioni sanitarie, genetiche etc.)



Responsabile  
privacy





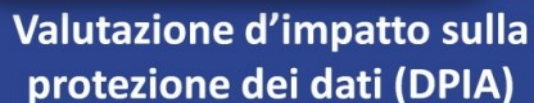
# Registro delle attività di trattamento (Art. 30)

- Il titolare o il suo rappresentante devono tenere un registro delle attività di trattamento sotto la propria responsabilità
- Contenuto
  - nome e dati del titolare del trattamento,
  - finalità del trattamento,
  - categorie di destinatari,
  - categorie di dati trattati,
  - durata del trattamento,
  - misure tecniche e organizzative in cui consiste il trattamento
  - misure di sicurezza adottate

- Qualora designato, il 'Data Protection Officer' deve operare una previa valutazione dei rischi
- È necessario
  - Quando c'è una valutazione estesa e sistematica degli aspetti personali delle persone fisiche basata su un processo automatizzato, inclusa la profilazione o su cui si basino decisioni in grado di produrre effetti giuridici sulle persone

A graphic element consisting of a red rounded rectangle with a faint background image of a document and a magnifying glass. The text 'Rischi per la privacy' is written in white, bold font. To the left of the rectangle, the text 'RGPD' is visible in blue, with 'REGOLAMENTO (UE) 2016/679' in smaller text below it.

**Rischi per la  
privacy**

A blue rectangular box containing the text 'Valutazione d'impatto sulla protezione dei dati (DPIA)' in white, bold font.

**Valutazione d'impatto sulla  
protezione dei dati (DPIA)**

## Privacy Impact Assessment: i criteri di redazione



Obbligo di PIA  
quando il  
trattamento:



Sentito il DPO, il Titolare nella PIA deve tener conto degli impatti del trattamento sui diritti dell'interessato in un'ottica di adempimento agli obblighi del Regolamento anche relativamente all'operato dei fornitori e dei sub-fornitori, tenuto conto dei Pareri dei WP29.

- la violazione sugli **obblighi del titolare** e del suo **rappresentante** (Artt. 24, 25 27, 28 e 32) è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente,





- La vendita di dati personali in base ad un trattamento illecito (per una **finalità diversa** da quella per la quale sono stati raccolti, **senza il previo consenso** dell'interessato) è punibile con la detenzione da 1 a 3 anni (Art. 167, 3 Cod. privacy).





UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

# Misure del Garante della privacy

Spogi

Dipartimento di Scienze Politiche,  
Giuridiche e Studi Internazionali

- In caso di urgenza il Garante della privacy può bloccare la vendita e ordinare che l'interessato sia informato dal titolare del trattamento e abbia una nuova possibilità di prestare il consenso



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI



# La Risoluzione del Parlamento europeo del 2019



- Il 4 aprile 2019 sull'**uso secondario** dei dati raccolti da parte delle istituzioni pubbliche
- Richiede la revisione della Direttiva 2003/98/EC
  - Inadeguata di fronte alle sfide sollevate dall'Intelligenza Artificiale
- Gli *open data* possono favorire il **mercato interno**
- Richiede il riconoscimento del principio dell'**'open data by design and by default'**
  - Protezione della sicurezza pubblica
  - Protezione delle infrastrutture sensibili
  - Protezione dei dati personali contro l'identificazione
  - Salute pubblica e sicurezza

L'accesso alle informazioni è un  
diritto fondamentale

Potenziale conflitto col principio  
della protezione dati 'by design'

regressivo



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

# Il caso *Tiziana Life Science*

Spogi

Dipartimento di Scienze Politiche,  
Giuridiche e Studi Internazionali

- Nel 2000 è stata fondata una ricerca sul DNA di una longeva popolazione di Tiscali

**citizen veillance**

- Una biobanca, SharDna, che conserva oltre 200.000 campioni biologici della comunità di Tiscali

**Processo penale per furto**

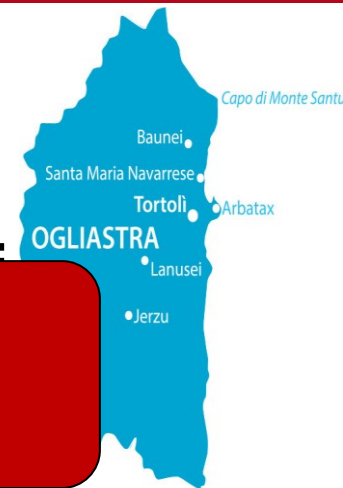
- I cittadini hanno avuto libero accesso ai servizi e hanno fornito ulteriori informazioni sul loro stato di salute

**Stop dal Garante della privacy**

- Nel 2009 SharDna è fallita e una nuova società, Life Science Plc l'ha acquistata per sviluppare farmaci

- Campioni biologici rubati e ritrovati all'estero

**Nuovo consenso libero e informato**



- Privacy nasce come diritto alla riservatezza e poi si è differenziata dal diritto alla protezione dei dati
- In Europa la privacy si è affermata prima a livello di Consiglio d'Europa poi a livello di Unione europea
- Nell'ambito dell'Ue il GDPR risponde all'esigenza di garantire l'uniformità del mercato a livello europeo
- Si articola sui principi dei Privacy by design e Privacy by default
- È un esempio di «governance rights based» unico a livello mondiale





UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

# Ultima lezione

Spogi

Dipartimento di Scienze Politiche,  
Giuridiche e Studi Internazionali

- Lunedì 1 giugno 8.40-10.20
- D. Ruggiu, A. Sitzia
- **Aula 1BC/45** Dipartimento di Matematica, via Trieste 63

**Il caso della  
«gamification»**





UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA



Dipartimento di Scienze Politiche,  
Giuridiche e Studi Internazionali

[daniele.ruggiu@unipd.it](mailto:daniele.ruggiu@unipd.it)