Privacy e Data Protection

Dati personali

- Dati che identificano o rendono identificabile una persona e possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, la sua salute, la sua situazione economica, …

- Sono particolarmente importanti:
  - Dati identificativi: quelli che consentono l'identificazione diretta, come i dati anagrafici (ad es. nome e cognome), foto …
  - Dati sensibili: quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale.
  - Dati giudiziari: quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari nel casellario giudiziale (ad esempio, le disposizioni penali di condanna, la liberazione condizionale, il divieto o l'obbligo di dimora, le misure alternative alla detenzione) o lo status di imputato o indagato.

Precedenti Normative sulla privacy

EUROPEAN UNION DATA PROTECTION DIRECTIVE

- Adottata nel 1998 dall'EU per:
  - garantire che gli Stati membri tutelassero i diritti fondamentali della privacy nel trattamento delle informazioni personali,
  - impedire agli Stati membri di limitare la libera circolazione delle informazioni personali all'interno dell'UE.

- La direttiva non era di per sé una legge, ma richiedeva agli Stati membri di emanare leggi che ne comprendessero i termini.

Precedenti Normative sulla privacy

Codice della privacy (Italia):

- *Legge sulla protezione dei dati personali (comunemente nota anche come Codice della Privacy) come disposizione della Repubblica Italiana, emanata con Decreto Legislativo 30 giugno 2003, n. 196.*

- I primi articoli riconoscono il diritto assoluto di ogni individuo sui propri dati, affermando che "Ogni persona ha diritto alla protezione dei dati personali che la riguardano".

- Lo scopo della normativa era quello di evitare che il trattamento dei dati avvenisse senza il consenso dell'avente diritto.

- A tal fine, il Titolo II, articoli da 8 a 10, ha definito i diritti degli interessati, le modalità di raccolta e i requisiti dei dati, gli obblighi di chi raccoglie, detiene e tratta i dati personali, la responsabilità e le sanzioni in caso di danni.

Normativa attuale sulla privacy

- **General Data Protection Regulation**
  - Regolamento con cui il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea intendono rafforzare e unificare la protezione dei dati per tutte le persone all'interno dell'Unione europea (UE).

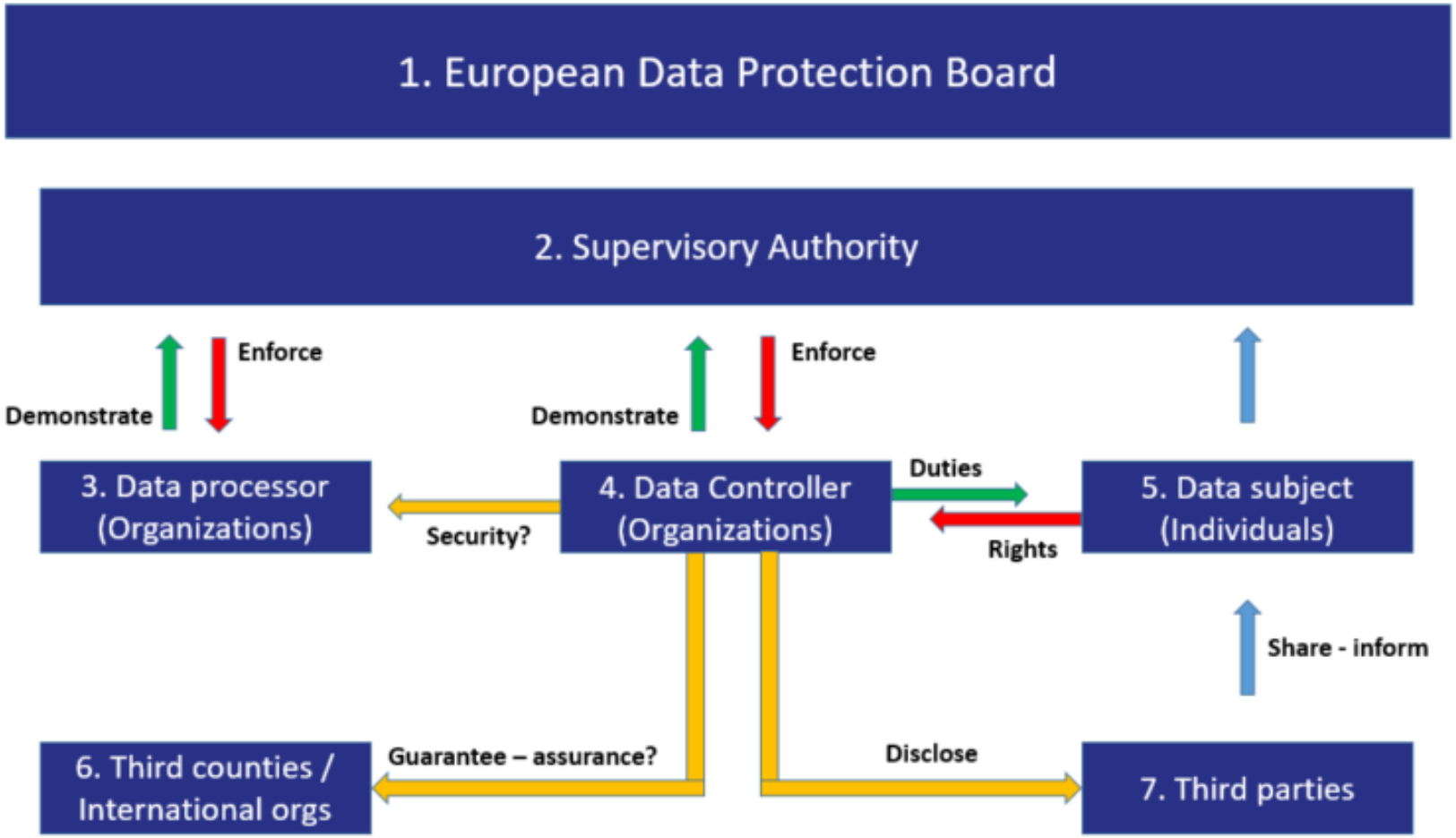
- In vigore dal **25 maggio 2018**

Dalla privacy alla data protection

privacy

data protection

Attori del GDPR



Comitato europeo per la protezione dei dati

- Il Consiglio è composto dal capo di un'autorità di controllo di ciascuno Stato membro e dal Garante europeo della protezione dei dati.

- Ruolo: esaminare ciò che funziona e ciò che non funziona e fornire consigli e indicazioni. Il Consiglio ha un Presidente

- Consultazioni tra la Commissione dell'Unione europea e il Consiglio di amministrazione.

Supervisory Authority

- Un'**autorità pubblica** indipendente istituita da qualsiasi Stato membro per far rispettare la legislazione a livello locale.
- Si assicura che il regolamento venga eseguito in ogni Stato.
- È responsabile dell'imposizione e della gestione delle sanzioni amministrative ai Controller e ai Processor.
- Deve coordinarsi con le altre Supervisory Authorities quando in una controversia o in un'azione ci sono più attori in più di uno Stato membro.

Data Processor

- Una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che **tratta i dati personali** per conto del Controller.
- I Data Processor non determinano le finalità e i mezzi del trattamento. Si limitano a trattare i dati come richiesto dal Controller.
- Ciò si verifica anche quando il trattamento dei dati è esternalizzato dal Controller e i dati sono trattati da una terza parte (ad esempio, un fornitore di servizi cloud).
- In base alla precedente direttiva, solo il Controller poteva essere sanzionato in caso di non conformità. Con la nuova normativa, **anche il Processor è responsabile**.

Data Controller

- Il Data Controller definisce quali dati personali servono all'azienda e per quali scopi.
- L'azienda richiede quindi questi dati alle persone (dipendenti, clienti, pubblico, ecc.).
- Il Data Controller è **responsabile** dell'osservanza del regolamento.
- Secondo la nuova legge, il Controller deve essere in grado di dimostrare la conformità in qualsiasi momento a seguito di una richiesta da parte della SA o dell'interessato (Data Subject).

Data Subject

- Il «data subject" è una persona fisica, un essere umano vivente.
- **Dati personali:** Qualsiasi informazione relativa a una persona fisica o «Data Subject», che può essere utilizzata per identificare direttamente o indirettamente la persona.
- Possono assumere diverse forme: un nome, una foto, un indirizzo e-mail, dati bancari, post su siti di social network, informazioni mediche o l'indirizzo IP di un computer.
- **Dati sensibili:** Informazioni che comprendono l'origine razziale o etnica dell'interessato, le sue opinioni politiche, le sue convinzioni religiose o altre convinzioni di natura analoga, la sua appartenenza a un sindacato, la sua salute fisica o mentale o le sue condizioni (compresi i dati genetici e biometrici), la sua vita sessuale e il suo orientamento sessuale, la commissione o la presunta commissione di un reato da parte sua, o qualsiasi procedimento per un reato da lui commesso o presunto tale, l'esito di tale procedimento o la sentenza di un tribunale in tale procedimento.

GDPR – Elementi chiave

- **Notifica di violazione**
  - Obbligatorio per qualsiasi violazione dei dati che possa "comportare un rischio per i diritti e le libertà delle persone".
  - Deve essere fatto entro **72 ore** dalla scoperta della violazione.
  - Gli incaricati del trattamento devono notificare i responsabili del trattamento "senza indebito ritardo" dopo essere venuti a conoscenza di una violazione dei dati.

- **Diritto di accesso**
  - Ottenere dal Controller la conferma che i dati personali di un cittadino sono trattati, dove e per quale scopo.
  - Il Controller deve fornire gratuitamente una copia dei dati personali in formato elettronico.

GDPR – Elementi chiave

- **Diritto all'oblio**
  - L'interessato può chiedere al titolare del trattamento di cancellare i propri dati personali, di cessare l'ulteriore diffusione dei dati e, potenzialmente, di far cessare il trattamento dei dati da parte di terzi.

- **Portabilità dei dati**
  - L'interessato ha il diritto di ricevere i propri dati personali in un "formato di uso comune e leggibile da dispositivo automatico" e ha il diritto di trasmettere tali dati a un altro responsabile del trattamento.

GDPR – Elementi chiave

- **Privacy by Design e by Default**
  - Inclusione della protezione dei dati fin dall'inizio della progettazione dei sistemi, piuttosto che come aggiunta.

- **Minimizzazione dei dati**
  - I Controller devono conservare e trattare solo i dati assolutamente necessari per l'espletamento delle loro funzioni.
  - L'accesso ai dati personali deve essere limitato a coloro che hanno bisogno di eseguirne il trattamento.

- **Sicurezza del trattamento**
  - I Controller e i Processor devono implementare misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio.

Data protection officer

- Obbligatorio solo per i Controller e Processor le cui attività principali consistono in operazioni di trattamento che richiedono il **monitoraggio regolare e sistematico dei data subject** su larga scala o di categorie particolari di dati, tra cui informazioni come i dati sanitari o le convinzioni religiose e politiche.

- Devono
  - essere nominato sulla base delle **qualità professionali** e, in particolare, delle conoscenze specialistiche in materia di legislazione e pratiche di protezione dei dati.
  - essere un **membro del personale** o un professionista **esterno**
  - disporre di **risorse** adeguate per svolgere i propri compiti e mantenere le proprie conoscenze specialistiche.
  - riferire direttamente al più alto livello di **gestione**.
  - non svolgere altri compiti che possano generare un **conflitto di interessi**.

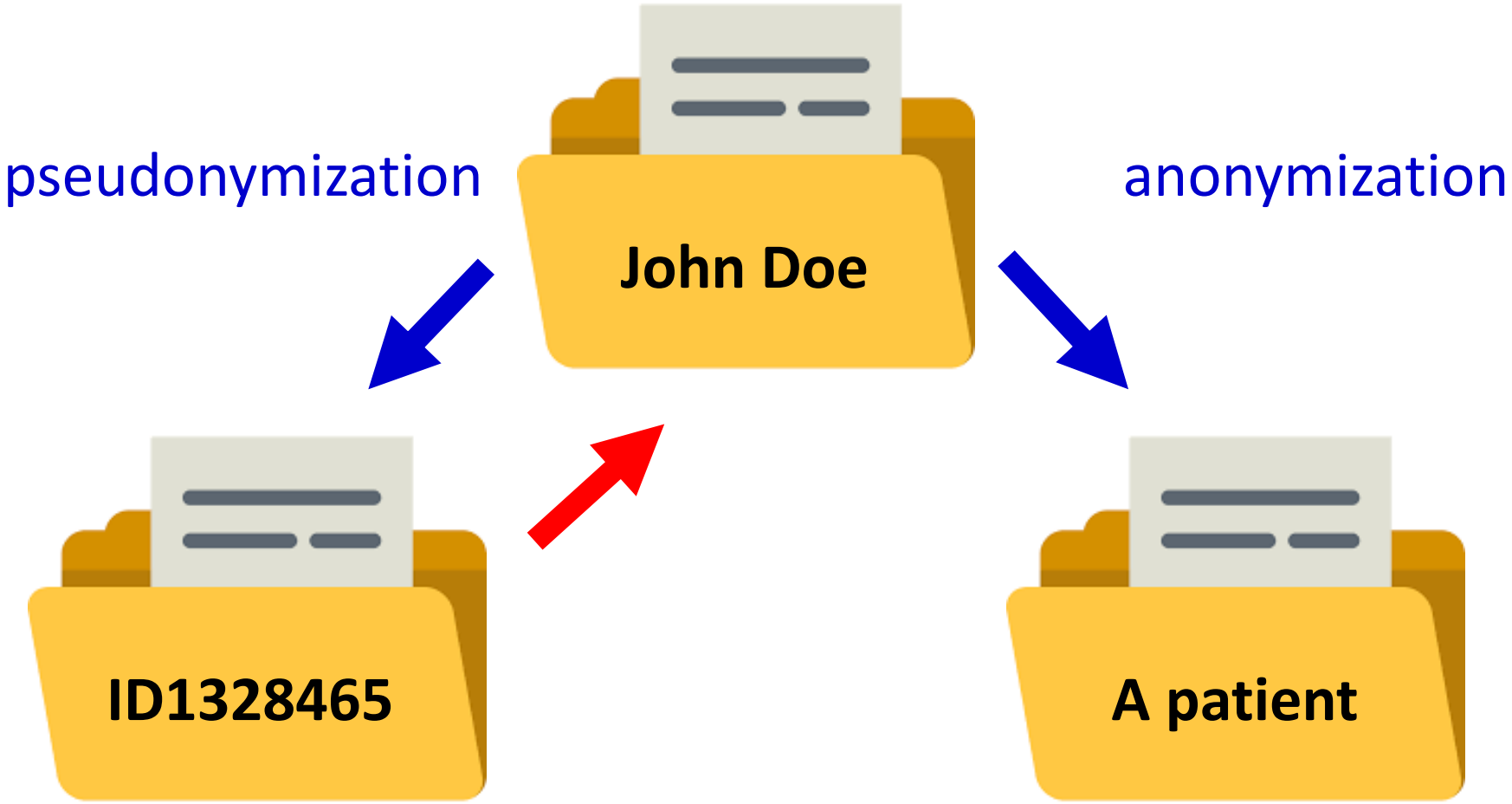
Pseudonymization / anonymization

- **Pseudonymization**:
  - Tecnica di gestione dei dati mediante la quale le informazioni personali all'interno di un record di dati sono sostituite da uno o più identificatori artificiali o pseudonimi.

- **Anonymization**:
  - Tecnica di gestione dei dati che li rende anonimi in modo tale che l'interessato non sia più identificabile e il GDPR non si applica ai dati anonimi.

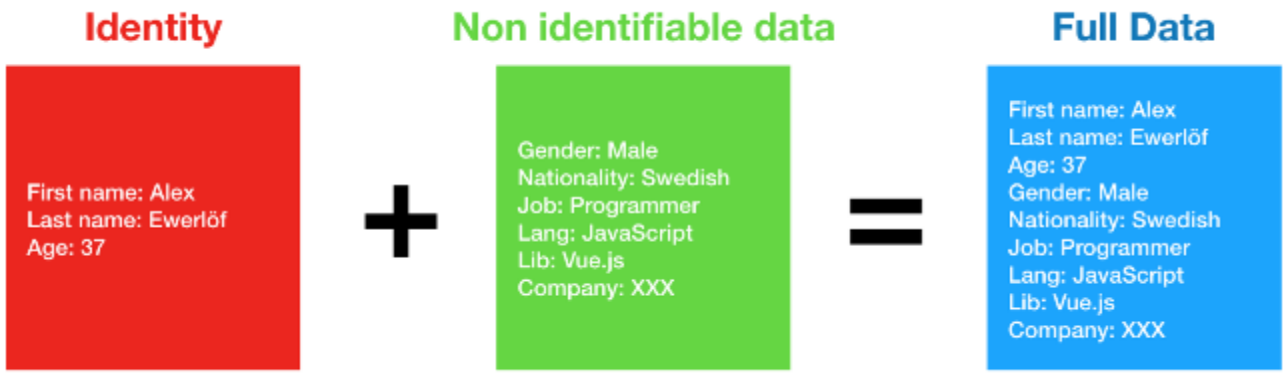
Name	Token/Pseudonym	Anonymized
Clyde	qOerd	xxxxx
Marco	Loqfh	xxxxx
Les	Mcv	xxxxx
Les	Mcv	xxxxx
Marco	Loqfh	xxxxx
Raul	BhQl	xxxxx
Clyde	qOerd	xxxxx

Pseudonymization / anonymization

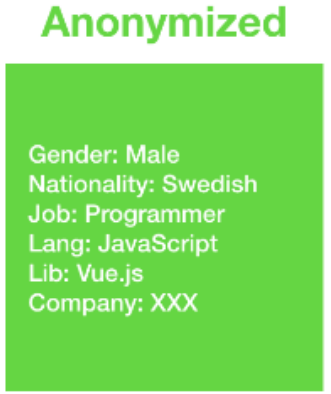


Pseudonymization / anonymization

- I dati pseudonimizzati possono comunque passare attraverso la reidentificazione per associarli nuovamente a un soggetto:



- Mentre i dati anonimi non possono essere re-identificati :



Pseudonymization

- **Scrambling**
  - Mescolando o offuscando le lettere, il processo può essere reversibile o meno.
- **Encryption** (symmetric)
  - Reversibile per chi conosce la chiave segreta (da conservare separatamente)
- **Masking**
  - Una parte importante/unica dei dati viene sostituita con caratteri casuali o altri dati (es. "5500 1234 9876 1204" → "5500 XXXX XXXX 1204").
- **Tokenization**
  - approccio non matematico che sostituisce i dati sensibili con sostituti non sensibili, denominati token.
- **Blurring**
  - Utilizza un'approssimazione dei valori dei dati (ad es. viso sfocato in un'immagine).

k-Anonymity

- Le informazioni di ogni soggetto non sono distinguibili da quelle di almeno altri *k*-1 individui
- Maggiore è il valore di *k*, più ambigua sarà la re-identificazione.
- Sia $RT(A\_1,\ldots,A\_n)$ una tabella e $\boldsymbol{QI}_{RT}$ un "quasi-identifier" ad essa associato. RT soddisfa il requisito di *k*-anonymity se e solo se ogni sequenza di valori nella tabella $RT[\boldsymbol{QI}_{RT}]$ appare almeno con almeno k occorrenze.
- Ciò si ottiene tramite generalizzazione, ovvero trasformando i valori del quasi-identifier in modo di essere meno specifici e non rappresentare più singoli individui.
- Il requisito di *k*-anonymity garantisce che un individuo può essere associato alla sua reale identità con una probabilità al massimo pari a 1/*k*.

k-Anonymity

	Race	Birth	Gender	ZIP	Problem
t1	Black	1965	m	0214*	short breath
t2	Black	1965	m	0214*	chest pain
t3	Black	1965	f	0213*	hypertension
t4	Black	1965	f	0213*	hypertension
t5	Black	1964	f	0213*	obesity
t6	Black	1964	f	0213*	chest pain
t7	White	1964	m	0213*	chest pain
t8	White	1964	m	0213*	obesity
t9	White	1964	m	0213*	short breath
t10	White	1967	m	0213*	chest pain
t11	White	1967	m	0213*	chest pain

Example of *k*-anonymity, where *k*=2 and QI={*Race*, *Birth*, *Gender*, *ZIP*}