# PSEUDONIMIZZAZIONE

UNIVERSITÀ DEGLI STUDI DI CATANIA
Marco Italia

# Sommario

# 1. Introduzione

La protezione dei dati rappresenta una preoccupazione centrale nel panorama contemporaneo dell'informatica e una questione critica per le società sempre più guidate dall'informazione. Negli ultimi anni, l'Unione Europea ha compiuto dei passi significativi in materia di protezione dei dati personali, tanto da essere tra le più all'avanguardia al mondo in contesti normativi nell'ambito di sicurezza dati e tutela della privacy.

Il presente documento è una sintesi ragionata delle informazioni tratte da fonti ufficiali e non con un focus al Regolamento UE 2016/679 (GDPR) [1] e al WP216 0829/14 [2]. L'obiettivo è duplice: sia quello di fornire un quadro teorico sul concetto di pseudonimizzazione, sia di proporre un'applicazione pratica di queste informazioni coerenti con i principi e sulle guide discusse.

Sebbene non sia il focus del documento, è presente un richiamo al tema dell'anonimizzazione, considerato solo in relazione alle similitudini nell'applicazione del trattamento di anonimizzazione e di pseudonimizzazione e alle tecniche di anonimizzazione utili alla pseudonimizzazione (vedi Generalizzazione).

# 2. Definizioni

È bene dare alcune definizioni dei termini più ricorrenti [1].

- Dato personale: qualsiasi informazione riguardante una persona identificata o identificabile.
- Interessato: persona identificata o identificabile di cui si hanno dati personali.
- Trattamento: qualsiasi operazione o insieme di operazioni, manuali o automatizzate, che sono applicate ai dati personali.
- Titolare del trattamento: la persona o organismo fisico o giuridico che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
- Responsabile del trattamento: la persona o organismo fisico o giuridico che tratta i dati personali per conto del titolare del trattamento[1].
- Destinatario: la persona o organismo fisico o giuridico che riceve comunicazione di dati personali, che si tratti o meno di terzi.
- Terzo: la persona o organismo fisico o giuridico che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.
- Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

[1] Considerata l'importanza del titolare del trattamento, e tenuto conto che il responsabile agisce su delega di quest'ultimo, da ora in avanti ogni riferimento alle scelte e agli obblighi relativi al trattamento dei dati si farà riferimento al titolare.

# 3. Dati anonimi e anonimizzazione

## 3.1 Generale

L'anonimizzazione è una tecnica applicabile ai dati personali per rendere l'identificazione delle persone fisiche impossibile da chiunque, incluso il titolare del trattamento, tenendo in considerazione l'insieme dei mezzi che allo stato attuale della tecnologia, possono essere ragionevolmente utilizzati[2].

Tale processo è irreversibile ed equivale alla cancellazione dei dati personali, ma richiede una continua attività di verifica e controllo, poiché le tecnologie e tecniche considerate oggi sicure potrebbero diventare obsolete o insufficienti nel giro di pochi anni.

Nel caso in cui, a seguito di una anonimizzazione efficace, non sia più possibile identificare l'interessato, il titolare del trattamento è tenuto a informarlo.

### 3.1.1 Principi necessari al trattamento dei dati

L'anonimizzazione, e qualunque altro trattamento di dati personali (come la pseudonimizzazione) deve rispettare i principi applicabili al trattamento di dati personali descritti nel GDPR [1]. Questi devono essere rispettati dal momento dell'acquisizione fino al momento dell'anonimizzazione o cancellazione. Se opportunamente anonimizzati, i dati anonimi non fanno più parte del GDPR[3].

- Liceità: il trattamento dei dati deve essere lecito, nelle misure descritte dall'articolo 6 del GDPR [1]; un aspetto particolarmente rilevante, sebbene non esclusivo, è il consenso esplicito e informato dell'interessato, raccolto dal titolare del trattamento.
- Correttezza: il trattamento deve svolgersi in modo equo e coerente con le legittime aspettative dell'interessato, garantendo il rispetto dei suoi diritti e la tutela della sua libertà personale.
- Trasparenza: il titolare è obbligato a fornire tutte le informazioni necessarie e relative al trattamento in forma concisa, trasparente, intellegibile e facilmente accessibile.
- Limitazione della finalità: i dati raccolti lecitamente devono essere successivamente trattati per scopi compatibili e connessi a tali finalità.
- Minimizzazione dei dati: i dati devono essere pertinenti, necessari e limitati rispetto alle finalità.
- Esattezza: i dati raccolti devono essere esatti. Se necessario, devono essere aggiornati tempestivamente.
- Limitazione della conservazione: i dati personali devono essere conservati per un arco di tempo non superiore a quello necessario alle finalità. È possibile conservarli più a lungo se archiviati in maniera sicura per finalità di pubblico interesse, ricerca scientifica o storica, o a fini statistici.
- Integrità e riservatezza: i dati devono essere trattati in modo da garantire un livello di sicurezza adeguato e devono essere protetti da trattamenti illeciti o non autorizzati, dalla perdita, dalla distruzione o da danni accidentali.
- Responsabilizzazione: il titolare del trattamento deve essere in grado di dimostrare che il rispetto dei principi applicabili al trattamento dei dati personali.

[2] Dal considerando (26) [1].
[3] È importante però notare che i dati hanno sempre il rischio di essere de-anonimizzati, per questo bisogna sempre capire se l'anonimizzazione effettuata è sufficiente.

### 3.1.2 Data protection by design and by default (DPbDD)

Per "Data Protection by design and by default" (DPbDD) [3] si intendono le misure di sicurezza tecniche appropriate che il titolare è tenuto ad applicare, non solo in riferimento ai dati, ma anche alla fase di progettazione, allo sviluppo e all'attuazione del trattamento.

In particolare, by Design sono le misure tecniche e organizzative adeguate a garantire il rispetto dei principi sopra descritti sin dalla fase di progettazione.
By Default comprende tutte le impostazioni operative (appunto predefinite) del trattamento, come la raccolta e l'utilizzo dei dati personali strettamente necessari per ciascuna finalità, limitandone l'accesso e la diffusione. Un esempio pratico del principio sono le policy del trattamento che il titolare definisce prima della raccolta dei dati.

### 3.1.3 Data Protection Impact Assessment

In presenza di trattamenti che comportano rischi elevati per i diritti e le libertà degli interessati, o che coinvolgono categorie particolari di dati (come quelli sanitari o giudiziari), è fortemente raccomandata, e in alcuni casi obbligatoria, la redazione di una valutazione d'impatto sulla protezione dei dati (DPIA) [4], ai sensi dell'art. 35 [1].
Tale documento consente di identificare precocemente le criticità e adottare misure tecniche e organizzative adeguate (tra cui la pseudonimizzazione) come possibile strumento di mitigazione del rischio.

## 3.2 Identificabilità dei dati anonimi e criticità

### 3.2.1 Quasi-identificatori

Gli identificatori diretti (o semplicemente identificatori) sono dati che permettono l'identificazione di una persona fisica senza ulteriori dati o conoscenze a priori. Esempi sono il nome e il cognome, codice fiscale o solo l'indirizzo di posta elettronica.

Di particolare rilevanza sono anche i quasi-identificatori [5], attributi che singolarmente non consentono l'identificazione di una persona, ma in combinazione tra loro o con altri dati presenti nella base di dati o esterni, rendono una persona fisica identificabile, o comunque riducono drasticamente il gruppo di possibili corrispondenze.
Un esempio sono la data di nascita, il sesso ed il CAP. Ciascuno di questi indica un gruppo ampio di persone, ma la loro combinazione permette di identificare un gruppo ristretto.

Sebbene gli identificatori debbano spesso essere eliminati, pseudonimizzati o nascosti in una tabella di corrispondenza come nel caso della pseudonimizzazione, i quasi identificatori possono risultare utili alle finalità del trattamento. Al fine di proteggerli, si ricorre alle varie tecniche di anonimizzazione (o a pseudonimizzazione), cercando però di preservare l'utilità informativa del dato.

## 3.3 Tecniche di anonimizzazione

Le varie tecniche di anonimizzazione hanno dei punti di forza e debolezza e la soluzione perfetta non esiste, in quanto queste vanno misurate in base al contesto, alla tipologia di dato e allo stato attuale della tecnologia.
Inoltre, le tecniche che seguono non vanno viste come esclusive, ma anzi vanno usate insieme quando possibile per rendere il trattamento più robusto.

### 3.3.1 Randomizzazione

La randomizzazione dei dati rappresenta una famiglia di tecniche di anonimizzazione che modificano l'esattezza del dato [2]. Proprio per questo motivo, la randomizzazione risulta sconsigliata in combinazione con la pseudonimizzazione, in quanto essendo dati personali devono essere esatti.

Tra queste tecniche, le più interessanti sono:

- Rumore statico: manipolando i dati con il rumore è particolarmente utile per mantenere la distribuzione generale. Ad esempio, si può aggiungere (o sottrarre) qualche anno di età (+-5) ai dipendenti di un'azienda per proteggere la loro identità.
- Permutazione: se nel rumore statico i dati vengono alterati in maniera casuale, nella permutazione i valori contenuti in un determinato campo vengono riassegnati a record diversi. Tuttavia, alcuni attributi sono però collegati fra di loro, e quindi perché la permutazione abbia successo è necessario che mantenga questi legami logici tra i dati.
  Ad esempio, età e salario aziendale. Se qualcuno di 27 anni avesse un salario molto alto, o la sua posizione aziendale fosse incompatibile con questo, un attaccante potrebbe intuire e ricostruire i dati originali con una certa accuratezza.

### 3.3.2 Generalizzazione

Questa famiglia di tecniche permette di mantenere l'esattezza del dato modificandone però il livello di dettaglio (ad esempio, invece della data di nascita si mantiene solo l'anno di nascita o un intervallo di età).
Questa manipolazione dei dati è particolarmente efficace se combinata con tecniche di pseudonimizzazione, in quanto si aggiunge un livello di incertezza maggiore all'individuazione, ed in certi casi, alla correlabilità.

Oltre alla generalizzazione che ho descritto, che è di effetto più immediato, esistono altre tecniche più raffinate di generalizzazione:

- Aggregazione e k-anonimato: queste tecniche di generalizzazione impediscono l'individuazione assicurando che ogni record sia raggruppato con almeno k altri record. Per far ciò, i valori interessati (spesso quasi-identificatori) vengono generalizzati, in modo da aumentare il numero di persone che condividono le stesse caratteristiche (estendendo l'esempio precedente, per l'età potrebbe essere usato un intervallo di dieci anni).
- l-l diversità: espande il k-anonimato in modo che in ciascuna classe di equivalenza abbia almeno l valori diversi, in modo da limitare la presenza di classi di equivalenza con scarsa variabilità di attributi.

# 4. Pseudonimizzazione

## 4.1 Generale

Le varie tecniche di pseudonimizzazione sostituiscono un identificatore (come nome e cognome) con uno pseudonimo identificativo (ad esempio un numero). In questo modo le persone interessate non possono essere identificate da chi è in possesso dei dati pseudonimizzati, ma solo da chi conosca anche quell'identificativo.

È infatti fondamentale che il titolare[4] protegga adeguatamente il segreto di pseudonimizzazione (o informazioni aggiuntive), ovvero l'elemento (come una chiave crittografica o una tabella di corrispondenza) che permette di ricostruire il legame tra pseudonimo e interessato[5].

### 4.1.1 Dominio di pseudonimizzazione

Un titolare che decida di applicare la pseudonimizzazione può definire un dominio di pseudonimizzazione [5]. Questo è il contesto in cui i dati, una volta pseudonimizzati, vengono trattati per estrarre informazioni utili alle finalità per le quali sono stati presi (ad esempio la gestione amministrativa) o per finalità compatibili, come quelle statistiche o di ricerca. È tuttavia fondamentale che il segreto di pseudonimizzazione venga tenuto separato dal dominio di pseudonimizzazione per non permettere l'identificazione.

Ad esempio: un'azienda di grandi dimensioni raccoglie i dati personali dei propri dipendenti per la gestione delle risorse umane. Dopo la pseudonimizzazione di questi dati, li invia a un reparto interno incaricato di condurre analisi statistiche sulle performance. Il segreto di pseudonimizzazione è tenuto separato, accessibile solo al personale autorizzato dal titolare, e non è disponibile all'unità che effettua le analisi. In questo esempio, il dominio di pseudonimizzazione è costituito dal contesto analitico.

Fanno parte del dominio anche eventuali soggetti terzi[6] che, per qualsiasi ragione, potrebbero accedere ai dati, sia che ciò avvenga su decisione del titolare, sia che si verifichi in modo non intenzionale (come in caso di perdita di dati o accesso non autorizzato).

### 4.1.2 Quando applicarla

La possibilità di identificare tramite il segreto di pseudonimizzazione gli interessati rende la pseudonimizzazione una tecnica di protezione particolarmente indicata nei contesti in cui il trattamento dei dati personali non richiede l'identificazione diretta e costante dell'interessato, ma in cui è comunque necessario preservare la possibilità di risalirvi in casi specifici, per finalità legittime, previste e documentate[7].

È quindi fondamentale quando il trattamento può condurre, anche in fasi successive, alla notifica individuale all'interessato (ad esempio comunicazioni sanitarie o di rischio) o ad una comunicazione a soggetti terzi (esempio autorità competenti o reparti interni autorizzati).

---

[4] Difatti solo i soggetti esplicitamente autorizzati possono avere accesso alle informazioni aggiuntive
[5] Più informazioni al capitolo 4.3 nelle tecniche di pseudonimizzazione.
[6] 2.3 (42) [5].
[7] In alcuni casi la pseudonimizzazione è richiesta dalla legge, come nel caso del trattamento di dati giudiziari o genetici per la legge italiana.

## 4.2 Tecniche di attacco

Prima di comprendere come proteggere i dati pseudonimizzati, risulta utile conoscere i principali motivi e le modalità attraverso cui tali dati possono essere violati [6]. Comprendere che rischi corrono e quali tecniche possono essere utilizzate per aggirare la pseudonimizzazione permette di valutare meglio l'efficacia delle misure adottate.

A tale scopo è bene descrivere le motivazioni degli attacchi:

- Recupero del segreto di pseudonimizzazione: può essere fatto sia tramite accesso non autorizzato o tramite deduzione del segreto.
- Re-identificazione: l'obiettivo è l'identificazione di uno o più interessati, e può avvenire anche senza conoscenza del segreto di pseudonimizzazione, tramite conoscenza esterna, sfruttando pattern rari nel database o ancora tramite linkage tra dataset.
- Attacco per discriminazione: con questo attacco non si mira alla de-anonimizzazione, ma a ottenere informazioni sensibili su interessati o su gruppi di interessati dai dati pseudonimizzati. (ad esempio, in un database medico potrebbe rivelare che un soggetto ha una malattia rara e la zona dove vive (CAP). Questo potrebbe bastare ad un attaccante, pur non avendo scoperto l'identità dell'interessato, a ricollegare la persona con lo pseudonimo).

L'efficacia degli attacchi varia in base a parametri, tra i quali:

- La quantità di informazioni riguardo gli interessati pseudonimizzati.
- Le informazioni pregresse dell'attaccante.
- La dimensione dell'insieme (o dominio) degli identificatori possibili.
- La dimensione del dominio di pseudonimizzazione.
- La funzione di pseudonimizzazione (e la conservazione e dimensione del segreto).

Nella descrizione delle seguenti tecniche, si assume che l'attaccante, interno o esterno al dominio di pseudonimizzazione, non abbia accesso alle informazioni aggiuntive necessarie al collegamento tra pseudonimi ed interessati. Sebbene la protezione di queste sia una criticità non trascurabile, essa non rientra nell'ambito di questo documento.

### 4.2.1 Brute force

La fattibilità di un attacco di brute force contro la pseudonimizzazione dipende dalla possibilità per l'attaccante di applicare la funzione di pseudonimizzazione (tramite conoscenze a priori o avere accesso a una "black box").

L'efficacia dell'attacco è legata alla limitatezza del dominio degli identificatori possibili: quanto più è ristretto, tanto più semplice per l'attaccante è provare tutte le combinazioni possibili finché non ottiene una corrispondenza tra pseudonimo e dato personale.
Se l'insieme è troppo grande (o non c'è alcun legame logico, come nel caso di pseudonimi generati casualmente), l'attacco è difficile o impraticabile.

### 4.2.2 Attacco dizionario

L'attacco dizionario rappresenta una forma evoluta dell'attacco brute force. L'attaccante invece di calcolare la funzione di pseudonimizzazione ogni volta, utilizza un dizionario precompilato di associazioni tra identificatori reali e pseudonimi. Questo dizionario viene generato utilizzando la stessa funzione di pseudonimizzazione applicata ai dati reali (ad esempio, una funzione hash nota).

### 4.2.3 Guesswork (Deduzione)

A differenza dei precedenti, questo tipo di attacco sfrutta conoscenze a priori e informazioni probabilistiche in possesso dell'attaccante per de-anonimizzare o dedurre l'identità di una persona. Ad esempio, se un attaccante è a conoscenza che nel dataset fornito è presente un individuo affetto da una malattia rara, saprà individuarlo con facilità, o quantomeno ridurre significativamente il numero di record compatibili.

## 4.3 Tecniche di pseudonimizzazione

Adesso che abbiamo un quadro chiaro delle strategie di attacco e di cosa gli attaccanti cercano di ottenere, vediamo alcune tecniche per proteggere i dati con la pseudonimizzazione. Tutte le tecniche analizzate sono, per semplicità nel descriverle, a singolo identificatore. Molte di queste trasformazioni possono però utilizzare più identificatori con pochi accorgimenti.

### 4.3.1 RNG

Il primo approccio, più semplice, per la pseudonimizzazione consiste nel sostituire l'identificativo con un numero generato casualmente. Il collegamento tra il numero generato e l'identificativo originale viene mantenuto in una tabella di corrispondenza (o lookup table), che in questo caso è il segreto di pseudonimizzazione.

Questo metodo, anche se semplice, risulta molto sicuro in quanto senza segreto di pseudonimizzazione non c'è modo di risalire dal numero all'identificativo. Però questa tecnica porta con sé due problemi: la scalabilità (bisogna conservare una tabella di corrispondenza che potrebbe essere molto grande) e le collisioni (in base all'implementazione).

### 4.3.2 Hash crittografico

Un altro approccio consiste nell'utilizzo di trasformazioni crittografiche. Con queste, il segreto di pseudonimizzazione risiede anche nell'algoritmo usato, in quanto un attaccante che scopre quale algoritmo è stato usato può tentare attacchi di brute force.

- Hash crittografico: famiglia di funzioni che prendono in input solo l'identificatore. È a senso unico e non ha collisioni. Questa famiglia di funzioni è generalmente ritenuta debole, in quanto prono ad attacchi brute force e dizionario (soprattutto se il dominio degli identificatori è limitato o conosciuto, ad esempio nomi o date).
- MAC: come l'hash crittografico, prende però in input sia l'identificatore sia una chiave, rendendo molto difficile gli attacchi di brute force.

Per rendere più robuste queste tecniche, può essere implementato l'utilizzo di salt.

### 4.3.3 Crittografia simmetrica a blocchi

Le funzioni crittografiche simmetriche permettono di ottenere uno pseudonimo a partire da un identificatore e viceversa, utilizzando una chiave segreta. Questa proprietà consente al titolare del trattamento di ricavare direttamente il dato pseudonimizzato e, se necessario, ripristinare l'identificatore originale, senza dover mantenere una tabella di corrispondenza tra identità e pseudonimi. Tale caratteristica rappresenta un vantaggio in termini di scalabilità e gestione sicura delle corrispondenze.

## 4.4 Implementazione e policy

Il titolare, in linea con i principi del DPbDD, predispone una policy prima ancora di iniziare la raccolta dei dati, [5] definendo in modo chiaro ogni fase del trattamento e accesso ai dati:

- Le finalità, ovvero perché stiamo raccogliendo i dati e quali dati è necessario raccogliere. È fondamentale tenere a mente i principi da rispettare durante tutte queste fasi.
- Redigere, se necessario, la valutazione d'impatto sulla protezione dei dati, così da individuare eventuali rischi elevati.
- Le modalità di raccolta dei dati specificando come e quando i dati vengono raccolti, e se è possibile applicare alcuni passi della pseudonimizzazione già dalla fase di raccolta.
- Quale trasformazione di pseudonimizzazione usare e come (quali identificatori trasformare; quali quasi-identificatori trattare poiché pericolosi; quali valori invece essenziali alle finalità e quindi lasciare invariati).
- Definire chi possa accedere al segreto di pseudonimizzazione e come proteggerlo.
- Definire il dominio di pseudonimizzazione e l'eventuale responsabile del trattamento (lo stesso titolare potrebbe ricoprire questa figura).
- Raccogliere i dati, applicare la trasformazione, conservare in modo sicuro il segreto di pseudonimizzazione e monitorare costantemente sia i dati trattati che lo scenario tecnologico per assicurarsi che le tecniche applicate siano ancora robuste.

# 5. Demo

Una start-up decide di creare un'applicazione sanitaria in grado, con l'IA e dei dati sugli utenti, di prevedere quando un utente possa avere l'insorgere un una malattia o quando questa possa aggravarsi.
Il titolare del trattamento, avendo dei dati con rischi elevati, esegue prima di tutto un DPIA [7].
Una volta compilato, bisogna decidere come proteggere i dati.
Il titolare decide di usare la pseudonimizzazione, così da poter contattare gli utenti in caso di emergenza (come la scoperta di una probabile emergenza sanitaria).
Il titolare, inoltre, sarà anche il responsabile del trattamento.

## Definizione della raccolta dati e dominio

Il passo successivo, prima di redigere una policy e definire il dominio e capire come raccogliere i dati.

1. I dati verranno raccolti tramite l'applicazione stessa. Nell'iscrizione gli utenti possono inserire delle visite effettuate (e le informazioni relative alle visite). Non appena inseriti, i dati vengono pseudonimizzati.
2. I dati sono utilizzati solo dall'applicazione e dall'IA, quindi il dominio di pseudonimizzazione è l'IA.

## Policy sul trattamento dei dati:

### *1. Finalità del trattamento*

Il presente trattamento prevede il processo di pseudonimizzazione dei dati personali sanitari a fini di ricerca, sperimentazione tecnica e training AI.

### *2. Tipologia di dati trattati*

I dati oggetto di pseudonimizzazione comprendono:

- Dati identificativi: codice fiscale, nome, cognome, sesso, data di nascita, CAP;
- Dati clinici: diagnosi, data diagnosi, trattamento, ospedale, reparto.

### *3. Tecniche di pseudonimizzazione*

La pseudonimizzazione viene eseguita tramite:

- UUID casuali / hash criptografici.

### *4. Conservazione dei dati*

- I dati identificativi e i dati pseudonimizzati sono conservati in file separati.
- I dati originali (non pseudonimizzati) verranno cancellati alla fine del trattamento di pseudonimizzazione.
- Nessun dato è trasmesso a terzi né condiviso internamente senza il consenso esplicito del titolare e degli interessati.
- Regolarmente vengono eseguiti backup. Solo il titolare ha accesso ai backup.

### *5. Accesso ai dati*

Solo il titolare e il responsabile del trattamento possono accedere ai dati originali, ai fini del trattamento.

- Nessuno, eccetto il titolare ed il responsabile della pseudonimizzazione, possono accedere a dati identificativi e ai dati clinici.
- Tutti gli accessi sono tracciati e documentati (logging).
- I segreti di pseudonimizzazione vengono protetti da crittografia e solo il titolare ed il responsabile può accedervi.

### *6. Futuri trattamenti*

Qualsiasi futuro trattamento su dati pseudonimizzati dovrà:

- Avvenire esclusivamente sui dati privi di identificativi diretti;
- Essere oggetto di una nuova valutazione d'impatto (DPIA) da parte del titolare;
- Seguire policy aziendali in linea con il Regolamento UE 2016/679 (GDPR).

### *7. Cancellazione*

Nel caso di cancellazione dei dati, gli utenti verranno informati.

# Riferimenti


[1] Parlamento e Consiglio dell'Unione Europea, «General Data Protection Regulation 2016/679,» 27 Aprile 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679.

[2] WP216, «Parere 05/2014 sulle tecniche di anonimizzazione (0829/14),» 10 Aprile 2014. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf.

[3] European Data Protection Board, «Data Protection by Design and by Default v2.0,» 20 Ottobre 2020. [Online]. Available: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[4] WP248, «Guidelines on Data Protection Impact Assessment (DPIA),» 4 Ottobre 2017. [Online]. Available: https://ec.europa.eu/newsroom/article29/items/611236/en.

[5] European Data Protection Board, «Pseudonymisation Guidelines,» 16 Gennaio 2025. [Online]. Available: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf.

[6] Enisa, Pseudonymisation techniques and best practices, Enisa, 2019.

[7] Azienda Regionale Coordinamento della Salute, «Modello DPIA sanità,» Giugno 2024. [Online]. Available: https://arcs.sanita.fvg.it/media/uploads/2024/06/27/Modello%20DPIA_v.%201.0%20dd.%2018.06.2024.pdf.