UNIVERSITÀ POLITECNICA DELLE MARCHE

DII Dipartimento di Ingegneria dell'Informazione

unimc

Data protection by design & by default nel Progetto DHEAL-COM

Buone pratiche per la redazione del Data Management Plan

Giacomo Cucchieri

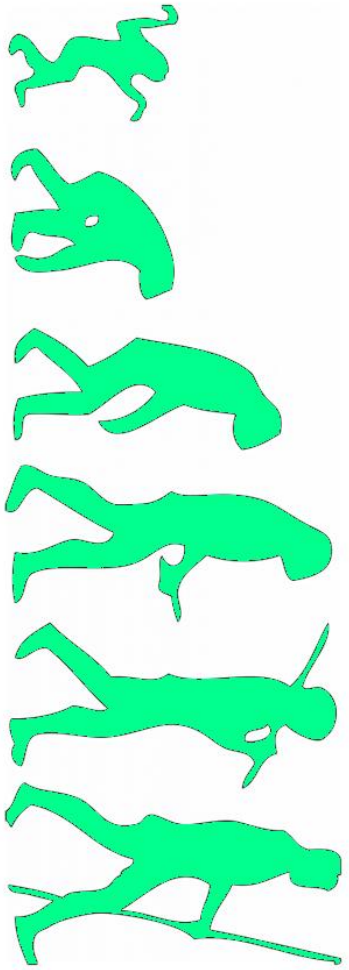
g.cucchieri@inrca.it

Giovedì 2 Ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Evoluzione Storica (1995-2025)

- **1995:** Ann Cavoukian (Ontario), nascita della Privacy by Design
- **2010:** Conferenza Internazionale Garanti (Gerusalemme), riconoscimento globale
- **2016:** GDPR, Art. 25 recepisce i principi PbD/PbDf
- **2018:** Entrata in vigore GDPR, obbligo in tutta l'UE
- **2020:** Linee guida EDPB per implementazione pratica
- **2022:** Prima sanzione a Meta per violazione Art. 25 (265M€)
- **2023:** ISO 31700, standardizzazione internazionale PbD
- **2024-2025:** Cyber Resilience Act e AI Act



Definizioni Chiave

Data protection by Design: «protezione incorporata»

- Built-in ≠ aggiunto dopo
- Integrazione della protezione dati a partire dalla fase progettuale, con approccio proattivo e preventivo, non correttivo

I **sette principi fondamentali** (Ann Cavoukian):

Definizioni Chiave

Data protection by Default: «configurazione predefinita sicura»

- Opt-in consapevole ≠ condivisione automatica, il silenzio NON è consenso
- Protezione per impostazione predefinita
- Configurazioni iniziali orientate alla privacy
- Principio di minimizzazione dei dati
- Solo dati necessari per la finalità specifica
- Tre **strategie chiave:**
  - Ottimizzare tramite analisi di quantità e qualità dei dati
  - Configurare le impostazioni controllabili dall'utente
  - Limitare i valori predefiniti privacy-friendly
- Nessuna azione esplicita richiesta all'interessato

Dalle definizioni ai check operativi

1. **Minimizzazione dati:** se non serve non chiedere il dato, o cancellarlo
2. **Crittografia di default:** niente caselle da spuntare per attivarla
3. **Accesso basato su ruoli:** permessi assegnati in base alle funzioni svolte
4. **Configurazione sicura di default:** a prova di errore umano
5. **Architettura decentralizzata:** database sensibili separati
6. **Consenso chiaro:** poche caselle, facili da gestire

Cambio di paradigma: da «privacy later» a «privacy first»

Articolo 25 GDPR: Struttura e Contenuti

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Articolo 25 del GDPR

Paragrafo 1 – *Protezione dei dati fin dalla progettazione*

- Obbligo di includere la **privacy** durante la progettazione tramite misure tecniche e organizzative adeguate
- Analisi dei rischi e redazione della **DPIA** quando necessaria (obbligatoria per trattamenti ad alto rischio, Art. 35 GDPR)
- Integrazione principi di **protezione** dei dati

Paragrafo 2 – *Protezione per impostazione predefinita*

- Raccolta dei **soli dati necessari** per la finalità del trattamento, il sistema deve essere il più tutelante possibile fin dal primo uso

Articolo 25 del GDPR

- **Minimizzazione automatica** dei dati e della possibilità di accedervi

Paragrafo 3 - *Meccanismi di certificazione volontari e approvati*

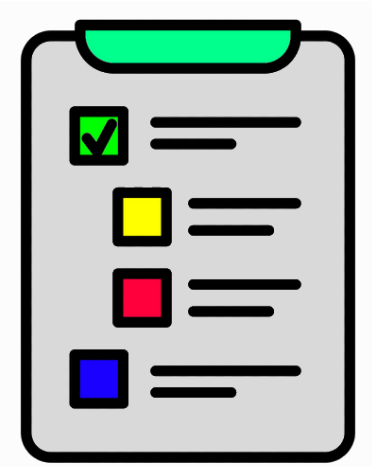
- Non obbligatori, ma utili per **dimostrare la conformità** alle misure richieste
- "La privacy non è un'aggiunta: è una funzione di progetto"

Data Management Plan e DPIA

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Data Management Plan (DMP)

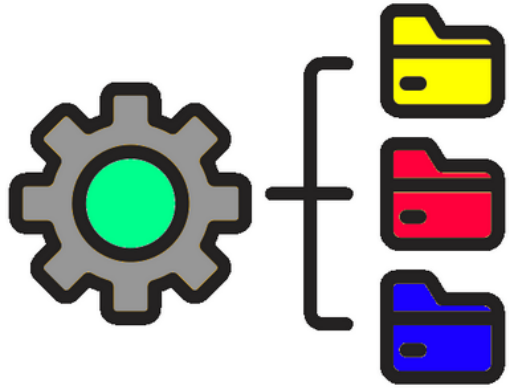
- Il **DMP** è un documento strutturato e «vivo»
- Permette di **pianificare proattivamente** la gestione dei dati
- Descrive **l'integrazione dei principi GDPR** in tutte le fasi:
  - progettazione raccolta dati
  - definizione misure di sicurezza
  - pianificazione conservazione e accesso
  - gestione consensi e diritti interessati
- Comprende la **valutazione dei rischi** e le relative misure di mitigazione
- Vale come **documentazione «trasparente»** (ovvero un'evidenza progettuale e operativa) per l'accountability



DMP: integrazione data protection

Elementi chiave nel DMP:

- pianificazione e **valutazione rischi ex-ante**, non correzioni ex-post
- **minimizzazione dati** dalla progettazione
- **misure di sicurezza** tecniche/organizzative, come la crittografia di default
- procedure di **accesso granulare**
- **consenso chiaro** e gestibile
- politiche di **conservazione** orientate agli obiettivi
- percorso di audit e **monitoraggio continuo**
- documentazione per **accountability dimostrabile**



Data Protection Impact Assessment (DPIA)

Definizione GDPR (Art. 35):

- valutazione preventiva dell'impatto sulla protezione dati
- obbligatoria quando il trattamento presenta «alto rischio»
- strumento di accountability per dimostrare compliance
  (ecco perché spetta al Titolare redigerla)

Quando è **obbligatorio:**

- …trattamento dati sanitari/biometrici su larga scala
- …utilizzo nuove tecnologie (AI, IoT, blockchain)

Sezioni principali:

- descrizione sistematica del trattamento e finalità
- valutazione necessità e proporzionalità
- identificazione e valutazione dei rischi
- misure di mitigazione e garanzie implementate

Data Protection Impact Assessment (DPIA)

Output previsto:

- documento di valutazione d'impatto completo
- piano di mitigazione dei rischi identificati
- eventuale consultazione con l'Autorità Garante (se il rischio residuo è alto)

Principi chiave:

- DPIA è un documento complementare al DMP che dimostra la privacy applicata («la privacy non deve essere solo una dichiarazione»)
- DPIA come approccio proattivo: valutare il rischio privacy prima di implementare
- DPIA in aggiornamento continuo: anche questo è un documento «vivo», allegato al DMP o comunque citato

Il progetto DHEAL-COM

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Il progetto

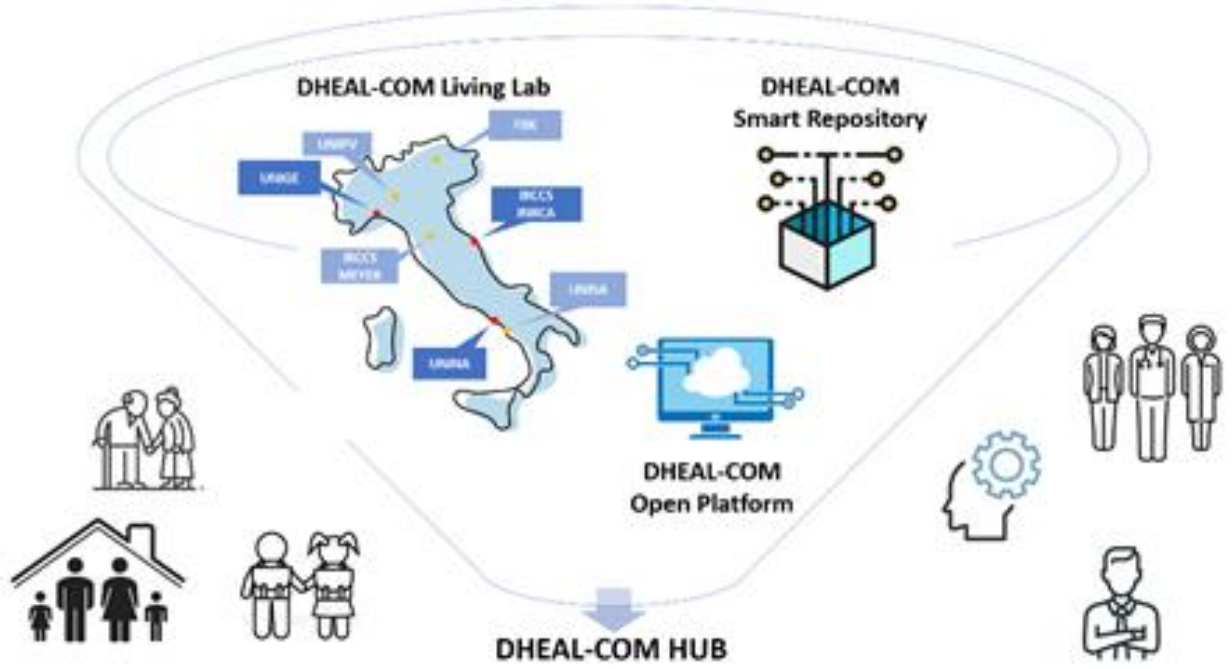
DHEAL-COM
Hub Life Science - Digital Health

- Un progetto di **ricerca tecnologica** che intende realizzare dei **prototipi di prodotti e servizi sanitari** ad alto contenuto digitale
- Un'**infrastruttura integrata** per l'innovazione nella **sanità digitale**, che include piattaforme cloud, repository di dati clinici e laboratori aperti
- **Gestione dati:** dataset clinici multi-istituzionali, condivisione sicura tra centri di ricerca, analisi integrate su grandi volumi

Obiettivi

Soluzioni sanitarie digitalizzate accessibili, per il **miglioramento** delle opportunità di **monitoraggio, gestione e trattamento del paziente** a domicilio o nelle strutture sanitarie di prossimità

- Open platform
- Smart repository, data lake
- Living labs



Partner e ambiti di ricerca

DHEAL-COM
Hub Life Science - Digital Health

- **IRCCS INRCA:** specializzazione geriatrica e invecchiamento
- **Università di Genova, Napoli, Salerno, Pavia:** ricerca accademica
- **Fondazione Bruno Kessler:** tecnologie innovative
- **Ospedale Pediatrico Meyer:** eccellenza pediatrica

Settori coinvolti: malattie neurodegenerative, digital health e IA sanitaria.

L'approccio è quindi multidisciplinare e multi-istituzionale.

INRCA Istituto di Ricovero e Cura a Carattere Scientifico
HEALTH AND SCIENCE ON AGING

Università di Genova

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

UNIVERSITÀ DEGLI STUDI DI SALERNO

UNIVERSITÀ DI PAVIA

FONDAZIONE BRUNO KESSLER

IRCCS Meyer
Azienda Ospedaliero Universitaria

Struttura del DMP per Dheal-com

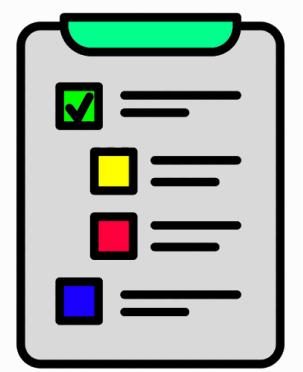
La **Milestone 1.3** del progetto riguarda la **stesura del DMP**, per il quale bisogna «*identificare e descrivere i dati che sono generati o raccolti, in accordo con le attività nel WP3 per la modellazione dei dati secondo lo standard HL7 e la specifica dei trattamenti, anche in base ai casi d'uso sviluppati*».

Dati trattati nel progetto: clinici, biometrici, comportamentali

Origine: pazienti, piattaforme, dispositivi vari

STRUTTURA

- Tipologia di dati e valutazione della sensibilità
- Misure privacy by design implementate
- Configurazioni by default adottate
- Pseudonimizzazione/anonimizzazione (Art. 89, trattamenti a fini di ricerca)

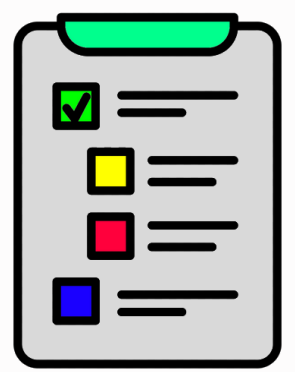


Struttura del DMP per Dheal-com

- Controlli accesso e separazione dei ruoli
- Backup sicuro e disaster recovery
- Procedura di risposta agli incidenti e notifica delle violazioni
- Formazione del personale e programmi di sensibilizzazione

Integrazione degli Art. 6/9 del GDPR nel DMP:

- specificare la base giuridica per ogni tipo di dato raccolto
- documentare il consenso e le modalità di raccolta
- prevedere misure per il trattamento dei dati sensibili (es. pseudonimizzazione, DPIA)
- inserire policy per il trattamento dei dati dei minori



DPIA nel Contesto Dheal-com

Trigger di obbligatorietà: trattamento dati sanitari su larga scala (Art. 35.3.b GDPR), collaborazione multi-istituzionale (complessità aumentata), utilizzo AI/ML per analisi predittive (nuove tecnologie), dataset longitudinali (trattamento sistematico nel tempo)

Processo strutturato per il DPIA:

- Definizione scopo e ambito trattamento
- Identificazione stakeholder e interessati
- Mappatura flussi dati inter-istituzionali
- Valutazione rischi privacy (probabilità × impatto)
- Misure mitigazione e controlli compensativi per ogni rischio
- Piano monitoraggio e review periodica

Coinvolgimento DPO e comitati etici dei partner

DPIA nel Contesto Dheal-com

I **quattro rischi principali** da identificare e mitigare:

1. **DPIA assente** o insufficiente
2. **Raccolta eccessiva di dati** non necessari
3. **Consensi pre-spuntati** o non chiari
4. **Sicurezza tardiva** con falle esposte

Tecnologie per la Data Security

- **Pseudonimizzazione:** sostituzione degli identificatori
  - Key management distribuito tra partner
  - Hash crittografici

- **Anonimizzazione:** cancellazione irreversibile delle identità

- **Cifratura end-to-end** per trasmissione e archiviazione, database mai in chiaro

Tecnologie per la Data Security

- **Controlli di accesso** basati su ruoli (RBAC) e **architettura decentralizzata**
  - Dataset sanitari separati per tipologia
  - «Se rubano una chiave rubano una stanza, non tutto l'edificio»

- **Architetture federate** per AI distribuita
  - Modelli condivisi, dati mai esposti
  - Tecniche di privacy differenziale per analisi aggregate

- **Calcolo multi-party** protetto
- Percorsi di **audit e logging** delle attività di accesso

Strategie di mitigazione e conclusioni

Strategie di mitigazione: dal mindset agli strumenti

Strumenti concreti:

- Privacy toolkit standardizzato e condiviso
- Librerie di modelli per interfacce conformi
- Rule engine che automatizza le regole

Governance organizzativa:

- Team privacy nel board decisionale
- Privacy champion per ogni partner Dheal-com
- Informazione trasversale e formazione continua
- Monitoraggio proattivo per mezzo di audit automatici e dashboard

«La privacy non è un settore, è un mindset»

Sfide e criticità nell'implementazione

Sfide culturali:

- privacy vista come ostacolo, non come valore
- «tolgo tempo allo sviluppo del prodotto a causa della privacy»

Sfide tecniche:

- dialogo difficile tra il nuovo sistema e il legacy
- interoperabilità opposta a segregazione dati

Sfide organizzative:

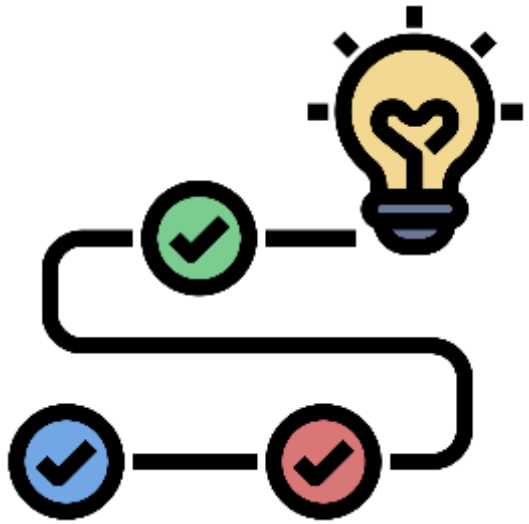
- coordinamento multi-istituzionale spesso complesso
- competenze per la privacy distribuite
- servizi terzi non controllati o non adeguati

«Cambiare mentalità: aumento della qualità grazie alla privacy»

CONCLUSIONI

- Data security by Design/Default: **da vincolo a vantaggio competitivo**

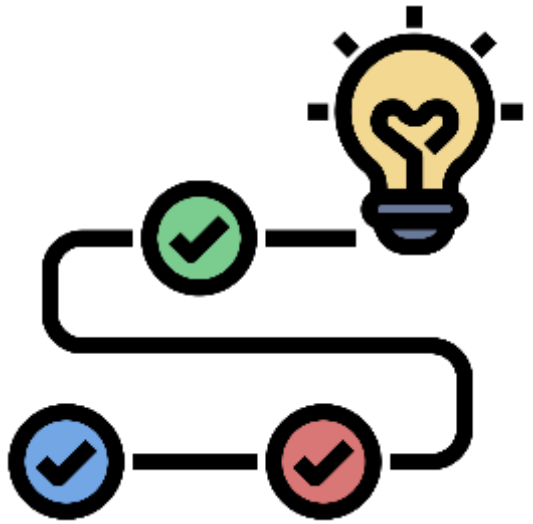
- **Dheal-com come paradigma per la sanità digitale etica:**
  - compliance verificabile e audit-ready
  - modello replicabile per la sanità digitale europea
  - standard di riferimento per ecosistemi sanitari



CONCLUSIONI

Per una buona riuscita del progetto, è necessario:

- Integrare la **protezione dati come valore progettuale**
- **Aggiornare il DMP** in modo dinamico, così che possa diventare uno strumento vivo e orientato alla fiducia
- **Far collaborare tutti i team**, tecnico legale e scientifico



Se vogliamo una sanità digitale davvero etica,
dobbiamo iniziare dai dati.

E iniziare bene, fin da subito.

GRAZIE