UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Il Quadro Normativo sulla Protezione dei Dati e il suo Impatto nella Redazione del DMP

Luca Antognoli
Direzione Scientifica
INRCA
l.antognoli@inrca.it

Giovedì 2 Ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

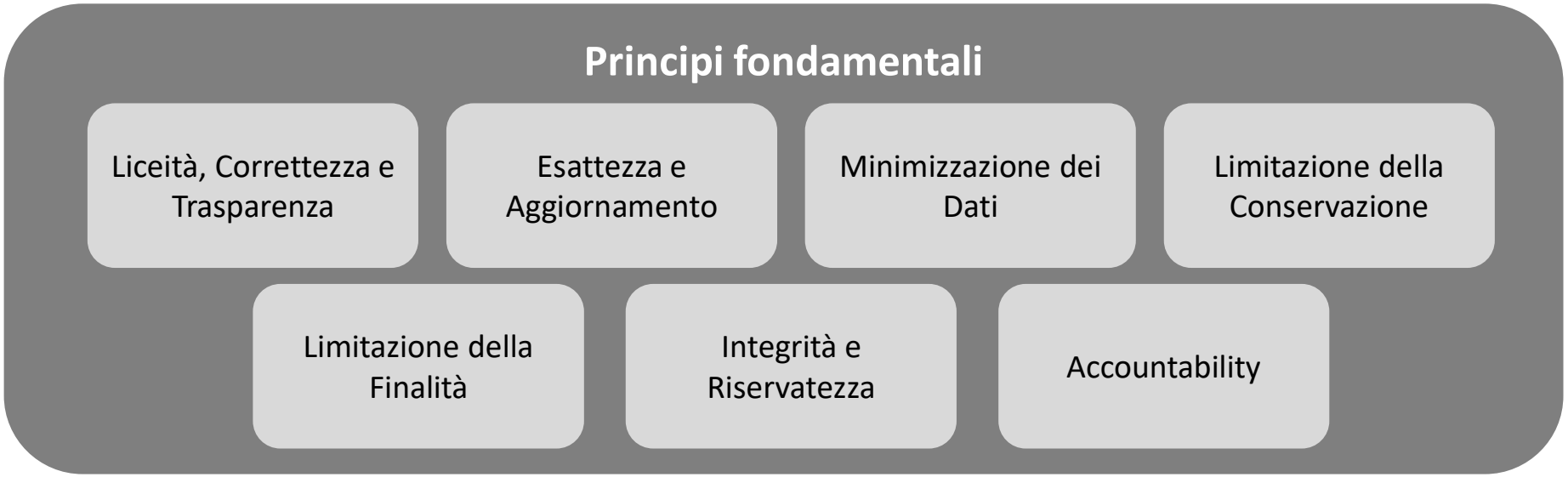
Il Quadro Normativo sulla Protezione dei Dati e il suo Impatto nella Redazione del Data Management Plan nel Progetto DHEAL COM

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

GDPR e principi chiave

Il Regolamento (UE) 2016/679 (GDPR) è una normativa europea direttamente applicabile dal 25 maggio 2018 in tutti gli Stati membri.

Scopo: Assicurare un uniforme ed elevato livello di protezione delle persone fisiche riguardo al trattamento dei dati personali e facilitare la libera circolazione di tali dati.



Normative complementari e specifiche

Codice Privacy italiano (D.Lgs. 196/2003 e aggiornamenti)

Integra e specifica il GDPR a livello nazionale garantendo una tutela rafforzata per i dati personali.

Include norme particolari per i dati sanitari, dati giudiziari e categorie speciali di dati.

Prevede lo svolgimento di valutazioni di impatto (DPIA) e discipina i dati trattati in ambito sanitario.

Direttiva NIS2 (Network and Information Security Directive) e DDL Cybersicurezza

Definisce obblighi per la sicurezza delle reti e sistemi informatici essenziali.

Il DDL Cybersicurezza italiano recepisce NIS2, introducendo responsabilità precise per enti pubblici e privati nell'adozione di misure tecniche e organizzative

Focus su gestione dei rischi, notifiche di incidenti, capacità di risposta e governance della sicurezza.

Data Governance Act UE (2022/868)

Normativa europea che facilita la condivisione sicura e responsabile dei dati tra enti pubblici, privati e tra Stati membri.

Promuove interoperabilità, qualità dei dati e governance trasparente.

Favorisce la realizzazione di ecosistemi dati che rispettino privacy e sicurezza.

Sicurezza e gestione dei dati in ambito sanitario

I **dati sanitari** sono considerati categorie speciali di dati personali e richiedono livelli di protezione più elevati rispetto ai dati comuni.

La loro natura sensibile impone requisiti stringenti per la **raccolta, trattamento, conservazione** e **condivisione**.

Privacy by design e by default

- Concetto introdotto dal GDPR che implica l'inclusione delle misure di protezione della privacy fin dalla progettazione dei sistemi e processi.
- Garantire che, per impostazione predefinita, siano trattati solo i dati strettamente necessari e protetti adeguatamente.

Obbligo di **notificare all'autorità garante** e agli interessati le violazioni di dati personali che comportano un rischio per i diritti e le libertà delle persone fisiche.

Procedure interne per la **gestione rapida ed efficace** degli incidenti.

Cifratura dei dati, **autenticazione** e **autorizzazione** degli accessi, backup periodici, monitoraggio e audit trail.

Importanza della **formazione** del personale e della definizione di responsabilità chiare.

DHEAL-COM
Hub Life Science - Digital Health

DHEAL-COM è un ecosistema che integra infrastrutture digitali, cloud, repository clinici e laboratori aperti per sviluppare e testare soluzioni innovative, favorendo il trasferimento tecnologico e l'accesso intuitivo nel settore sanitario

Medicina di prossimità

Creazione di un infrastruttura per supportare lo sviluppo di tecnologie innovative nella medicina di prossimità

Smart Repository

Infrastruttura sicura per il monitoraggio della salute e supporto alla sperimentazione di soluzioni tecnologiche

Open Lab

Laboratori dedicati alla sperimentazione e prototipazione di soluzioni sanitarie digitali

Piattaforma

Infrastruttura cloud dinamica accessibile a cittadini stakeholder per l utilizzo di strumenti software sanitari

Università di Genova

INRCA Istituto di Ricovero e Cura a Carattere Scientifico

Meyer Azienda Ospedaliera Universitaria

Università di Pavia

Università degli Studi di Napoli Federico II

Fondazione Bruno Kessler

Università degli Studi di Salerno

Piattaforma DHEAL-COM

Si presenta come un'infrastruttura cloud dinamica accessibile sia ai cittadini che agli stakeholder, tra cui laboratori di ricerca, IRCCS, medici, ospedali, operatori sanitari territoriali, professionisti sanitari, ricercatori, sistemi sanitari regionali, start-up ed imprese.

Servizi: Ecosistema integrato con infrastrutture digitali, repository clinici e laboratori aperti per sperimentazione e prototipazione soluzioni innovative.

Modelli: Strutture concettuali e pratiche che orientano l'integrazione e l'applicazione delle soluzioni tecnologiche digitali, facilitando l'interazione tra sistemi e l'efficacia delle soluzioni implementate.

Tecnologie: Strumenti, piattaforme digitali, infrastrutture cloud e processi innovativi sviluppati per facilitare la gestione, l'analisi dei dati, migliorando l'erogazione e la qualità dei servizi per la salute.

Progettazione Partecipata: Collaborare alla progettazione con tutti gli attori coinvolti, inclusi utenti finali, stakeholder, esperti e progettisti, per dare un contributo attivo al processo decisionale del progetto DHEAL-COM.

Implicazioni sul DMP per DHEAL-COM

La redazione del Data Management Plan (DMP) nel contesto DHEAL-COM deve:

- Dettagliare i flussi, le tecniche di raccolta e i standard di accesso e riuso dei dati sanitari, con particolare attenzione alla pseudonimizzazione e all'anonimizzazione per conformità GDPR.
- Integrare gli obblighi di protezione, archiviazione e backup, pianificazione dei privilegi di accesso e conservazione sicura secondo le direttive europee e nazionali.
- Descrivere le misure etiche adottate per garantire la sicurezza e l'interoperabilità dei dati, specificando le modalità di trattamento nei casi di ricerca e condivisione tra partner e con enti pubblici.
- Adeguare il piano alle novità normative come il Data Governance Act UE 2022/868 e il Codice Privacy, soprattutto nella gestione di dati sensibili e nelle procedure di consenso informato.

Impatti normativi sulla redazione del DMP

- Il GDPR influenza direttamente la struttura e i contenuti del DMP, richiedendo particolare attenzione alla classificazione dei dati personali, in particolare quelli sanitari (categorie speciali secondo art. 9 GDPR).
- Obbligo di definire chiaramente le modalità di raccolta, trattamento e conservazione, garantendo il consenso informato e i diritti degli interessati.
- Tracciabilità e documentazione dettagliata dei flussi e dei processi di trattamento dati.

- Il DMP deve descrivere le misure tecniche (es. cifratura, autenticazione, backup) e organizzative (policy, formazione, ruoli) implementate per proteggere i dati.
- Identificazione chiara dei responsabili della sicurezza, del monitoraggio e della risposta agli incidenti (es. Data Protection Officer e team di cybersecurity).
- Garantire coerenza con il principio di accountability previsto dal GDPR.

- Oltre al GDPR, si devono rispettare le disposizioni del Codice Privacy italiano (D.Lgs. 196/2003 e successive modifiche), che rafforzano la protezione dei dati sanitari.
- Considerare anche regolamenti e linee guida specifiche del settore sanitario, che possono richiedere ulteriori obblighi per la protezione e gestione dei dati (es. gestione dati sanitari, cartelle cliniche elettroniche).

Impatti normativi sulla redazione del DMP

Data Governance Act (DGA) favorisce la condivisione sicura, responsabile e trasparente dei dati, incentivando l'interoperabilità e la qualità dei dati trattati.

Il DMP deve prevedere meccanismi e standard per garantire che i dati siano facilmente utilizzabili tra enti diversi, mantenendo la riservatezza e la sicurezza.

Direttiva NIS2 e DDL Cybersicurezza Rafforzano gli obblighi di sicurezza digitale, imponendo misure proattive di gestione del rischio informatico.

Il DMP deve includere procedure per il monitoraggio continuo, la gestione e la notifica degli incidenti di sicurezza.

Necessaria una chiara definizione di ruoli e responsabilità per la cybersecurity, integrando team e figure dedicate.

Aggiornamento e sostenibilità del DMP

Il DMP non è un documento statico: deve essere regolarmente aggiornato in risposta a cambiamenti normativi, evoluzione tecnologica o nuove esigenze progettuali.

Garantire la sostenibilità nel medio-lungo termine della gestione dati, con pianificazione di risorse, formazione e controllo qualità.

Promuovere la trasferibilità e replicabilità del modello DMP su altre realtà sanitarie territoriali.

Linee guida operative per il DMP nel progetto DHEAL-COM

Tipologie di dati coinvolti (personali, sanitari, anonimizzati)

- Descrizione dei flussi di raccolta, conservazione, accesso e riuso
- Misure di sicurezza adottate: cifratura, controllo accessi, backup, audit trail
- Modelli di governance con ruoli e responsabilità ben definiti

Gestione del consenso e coinvolgimento stakeholder

- Importanza del consenso libero, specifico e informato
- Coinvolgimento attivo di cittadini, caregiver, professionisti e partner
- Trasparenza e comunicazione continua sui trattamenti dati

Monitoraggio, aggiornamento e miglioramento continuo

- Verifica periodica della conformità del DMP
- Aggiornamento costante in base a normative e tecnologie in evoluzione
- Strumenti di reporting e audit per garantire qualità e sicurezza

DMP IMPLEMENTATION WORKFLOW

- •Tipologie dati
- •Flussi dati
- •Sicurezza
- •governance

- •Consenso informato
- •Coinvolgimento attivo
- •trasparenza

- •Misure sicurezza
- •Deploy sistemi
- •Formazione

- •Verifica conformità
- •Audit sicurezza
- •Reporting

- •Analisi gap
- •Aggiornamenti normativi
- •Evoluzione tecnologica

GDPR Art. 30 (Registro trattamenti)

Codice Privacy Art. 110-116 (Dati sanitari)

GDPR Art. 7-9 (Consenso categorie speciali)

Codice Privacy Art. 23, 130

GDPR Art. 25 (Privacy by design)

Codice Privacy Art. 32-36 (Misure minime)

GDPR Art. 35 (DPIA)

DDL Cybersicurezza (Incident response)

Data Governance Act

NIS2

DDL Cybersicurezza

GRAZIE DELL’ ATTENZIONE