EHDS e Data Governance: Verso un’Europa della Condivisione dei Dati Sanitari

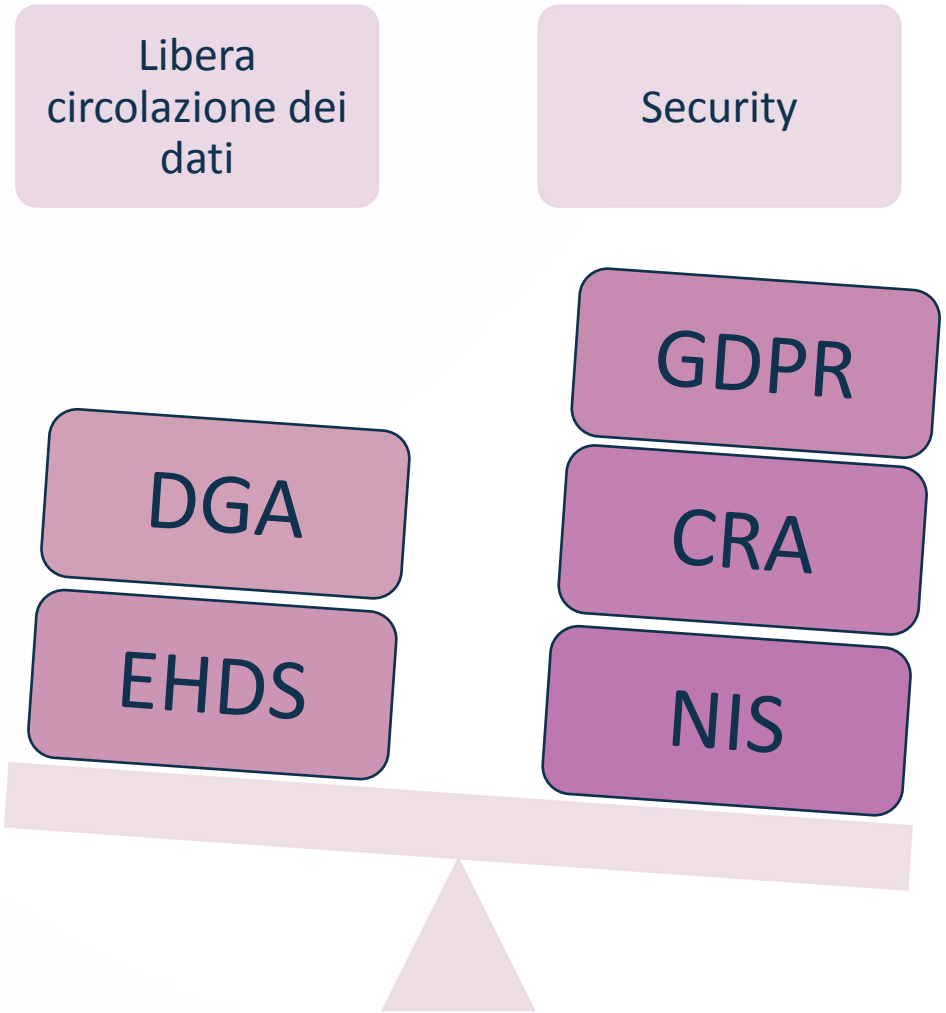
Nadina Foggetti

CNR-IBIOM
ELSI Officer - Elixir IT

Indice

Cos'è la sovranità digitale e perché è importante?

Il quadro giuridico



La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali".

Un Mercato Unico dei Dati per la Sovranità Digitale Europea: Il Data Governance Act (DGA)

Riuso dei dati personali e non

- Compliance
- Anonimizzazione e consenso
- Supporto dagli organismi competenti

Data Sharing services

- Condividere i dati soggetti/titolari e utenti
- Notifica alle autorità competenti
- Supervisione

Data Altruism

- Dati resi volontariamente ai fini del riuso per obiettivi di interesse generale
- Registrazione volontaria dei providers

Data altruism: in law

L’art. 2, par. 1, n. 16) DGA

«la condivisione **volontaria** di dati sulla base **del consenso accordato dagli interessati al trattamento dei dati personali** che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l’uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l’assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l’agevolazione dell’elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l’elaborazione delle politiche pubbliche o la ricerca scientifica nell’interesse generale».

Data altruism: in law

Art. 4 Divieto di accordi di esclusiva

1. Sono vietati gli accordi o altre pratiche relativi al riutilizzo di dati detenuti da enti pubblici e comprendenti le categorie di dati di cui all'articolo 3, paragrafo 1, che concedono diritti esclusivi o che hanno per oggetto o per effetto di concedere tali diritti esclusivi o di limitare la disponibilità di dati per il riutilizzo da parte di entità diverse dalle parti di tali accordi o altre pratiche.
2. In deroga al paragrafo 1, può essere concesso un **diritto esclusivo di riutilizzo dei dati di cui a tale paragrafo nella misura necessaria alla fornitura di un servizio o di un prodotto di interesse generale** che non sarebbe altrimenti possibile.

Data Altruism: in action

possibilità concreta di operare una “condivisione volontaria di dati”

sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano,

autorizzazioni di altri titolari dei dati

senza la richiesta o la ricezione di un compenso, per obiettivi di interesse generale previsti per legge nazionale (ad es. l'assistenza sanitaria)

Comitato europeo per l'innovazione in materia di dati

Ruolo di AGID

Aspetti di criticità

Qualificazione di “interesse generale”

Frammentarietà sanzionatoria

compatibilità tra tale attività e le cautele irrinunciabili previste dal GDPR in favore dei soggetti interessati

Quadro giuridico di riferimento

EHDS

HDS Regulation

L'European Health Data Space (EHDS) rappresenta una svolta nella gestione e condivisione dei dati sanitari in Europa. Con la pubblicazione in Gazzetta Ufficiale dell'UE del Regolamento (UE) 2025/327, l'EHDS diventa ufficialmente operativo, ponendo nuove sfide e opportunità per aziende, strutture sanitarie e cittadini.

Questo progetto ambizioso mira a migliorare l'accesso ai dati sanitari tra gli Stati membri, garantendo allo stesso tempo sicurezza, privacy e interoperabilità.

FAQ EHDS – 5 marzo 2025

Obiettivi

A ricercatori, innovatori e responsabili delle politiche sanitarie di utilizzarne alcune particolari categorie per finalità specifiche di interesse generale

All’individuo di controllare i propri dati sanitari elettronici;

Creare uno spazio comune in cui si garantisca:

EHDS – collegamenti con altre proposte legislative e iniziative

GDPR
EHDS si basa sui diritti previsti dal GDPR e ne sviluppa ulteriormente alcuni.

Unione Europea della Salute
L'EHDS rafforzerà il lavoro del Piano europeo contro il cancro, di HERA e della Strategia farmaceutica per l'Europa.

Data Governance Act, Data Act
L'EHDS integra e fornisce regole più specifiche per il settore sanitario.

Regolamento sull'Intelligenza Artificiale
L'EHDS supporta e integra la formazione dell'IA, l'interoperabilità tra IA e sistemi di cartelle cliniche elettroniche (EHR) e la qualità dei dati.

Quadro UE per la cybersicurezza (Direttiva NIS)
L'EHDS integra e fornisce regole più specifiche per il settore sanitario.

Regolamenti sui Dispositivi Medici
Se i produttori dichiarano l'interoperabilità dei dispositivi con i sistemi EHR, si applicano i requisiti dell'EHDS.

Basi giuridiche e ambito di applicazione

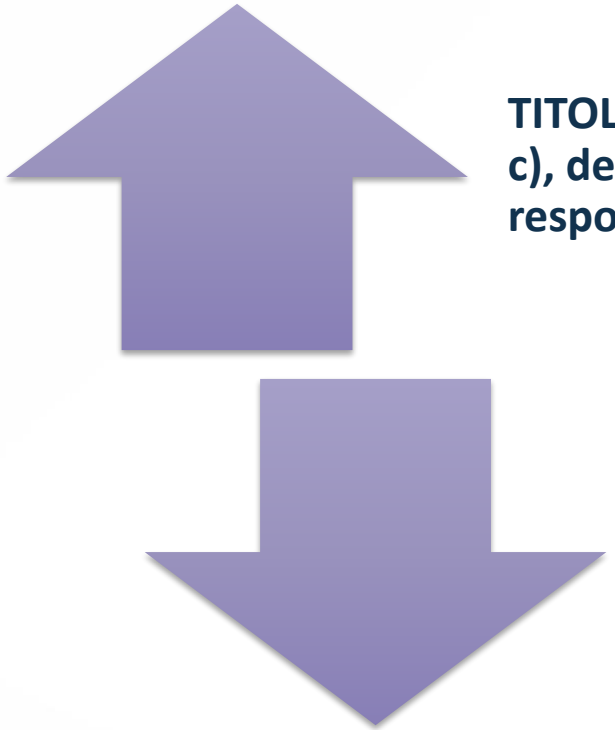
Base giuridica – Articolo 16 TUE e Articolo 114 TUE

- **Articolo 16** – L'EHDS si basa sul GDPR, rafforzando i diritti alla protezione dei dati personali sanitari e sfruttando le possibilità offerte dal diritto dell'UE per il trattamento dei dati sanitari sensibili e genetici.
- **Articolo 114** – L'EHDS ha l'obiettivo di migliorare il funzionamento del mercato interno e la libera circolazione di beni e servizi, evitando la frammentazione legislativa nel mercato interno e le diverse regole e pratiche tra gli Stati membri dell'UE.
- **Pieno rispetto dell'Articolo 168 TUE** – L'EHDS non interviene nell'organizzazione e nella fornitura dei servizi sanitari e delle cure mediche degli Stati membri.
- **Dati sanitari personali e non personali inclusi nell'ambito**.

EHDS: Basi giuridiche

Regolamento EHDS fornisce «*la base giuridica in conformità dell'art. 9, par. 2, lett j), del regolamento (UE) 2016/679 per l'uso secondario dei dati sanitari, stabilendo le garanzie per il trattamento, in termini di finalità legittime, una governance affidabile per fornire l'accesso ai dati sanitari (attraverso organismi responsabili dell'accesso ai dati sanitari) e il trattamento in un ambiente sicuro, nonché modalità per il trattamento dei dati, stabilite nell'autorizzazione ai dati*» (considerando 37).

Segue basi giuridiche



TITOLARE: obbligo giuridico ai sensi dell'art. 6, co. 1, lett. c), del GDPR di comunicare i dati agli organismi responsabili dell'accesso ai dati sanitari;

ORGANISMI RESPONSABILI DELL'ACCESSO : hanno compiti di interesse pubblico ai sensi dell'art. 6, co, 1, lett. e) GDPR («il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento»)

Uso primario

Solo le persone autorizzate possono accedere ai dati individuali.

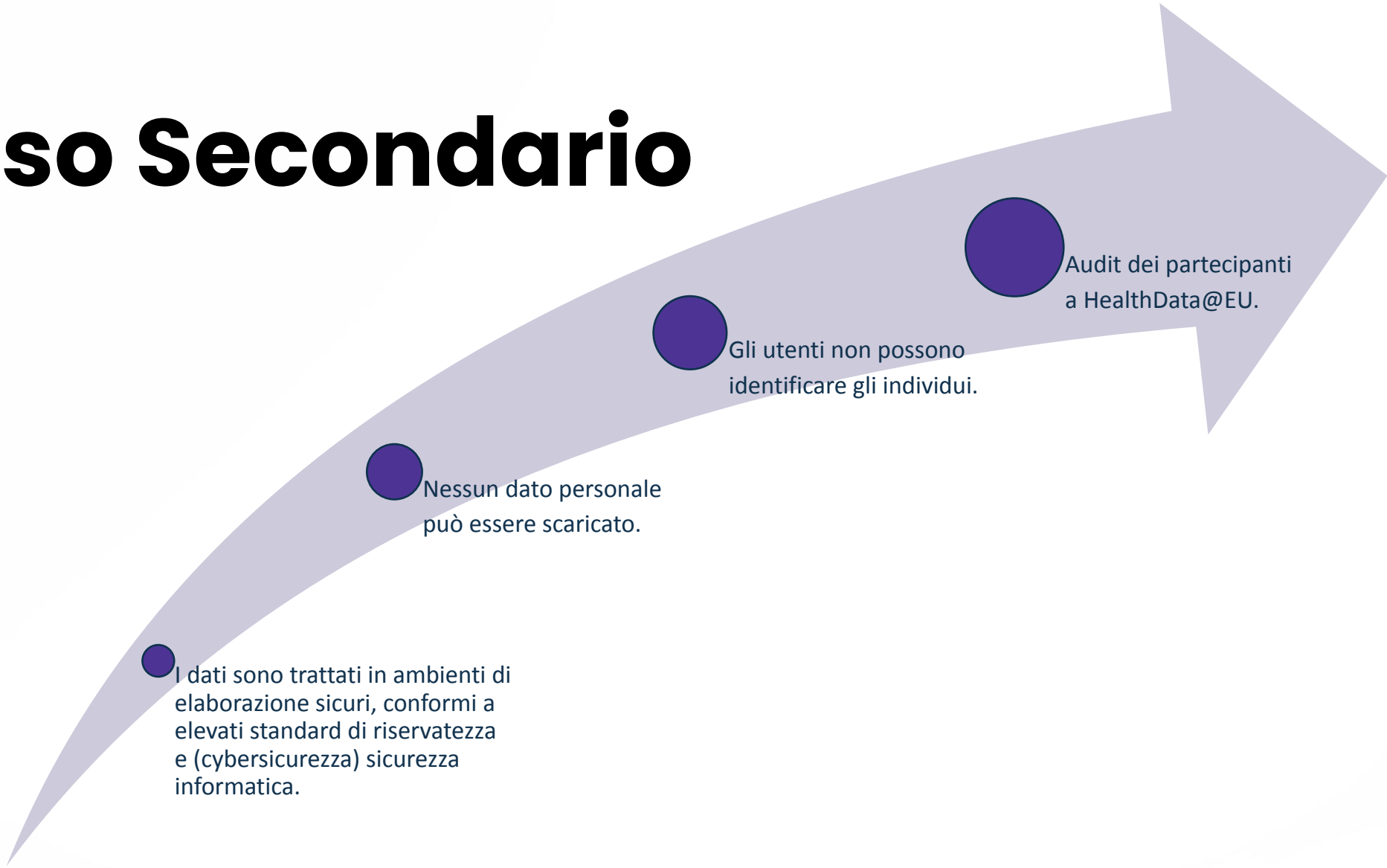
Autenticazione forte per pazienti e professionisti sanitari

Audit di sicurezza per l'infrastruttura MyHealth@EU (uso primario)

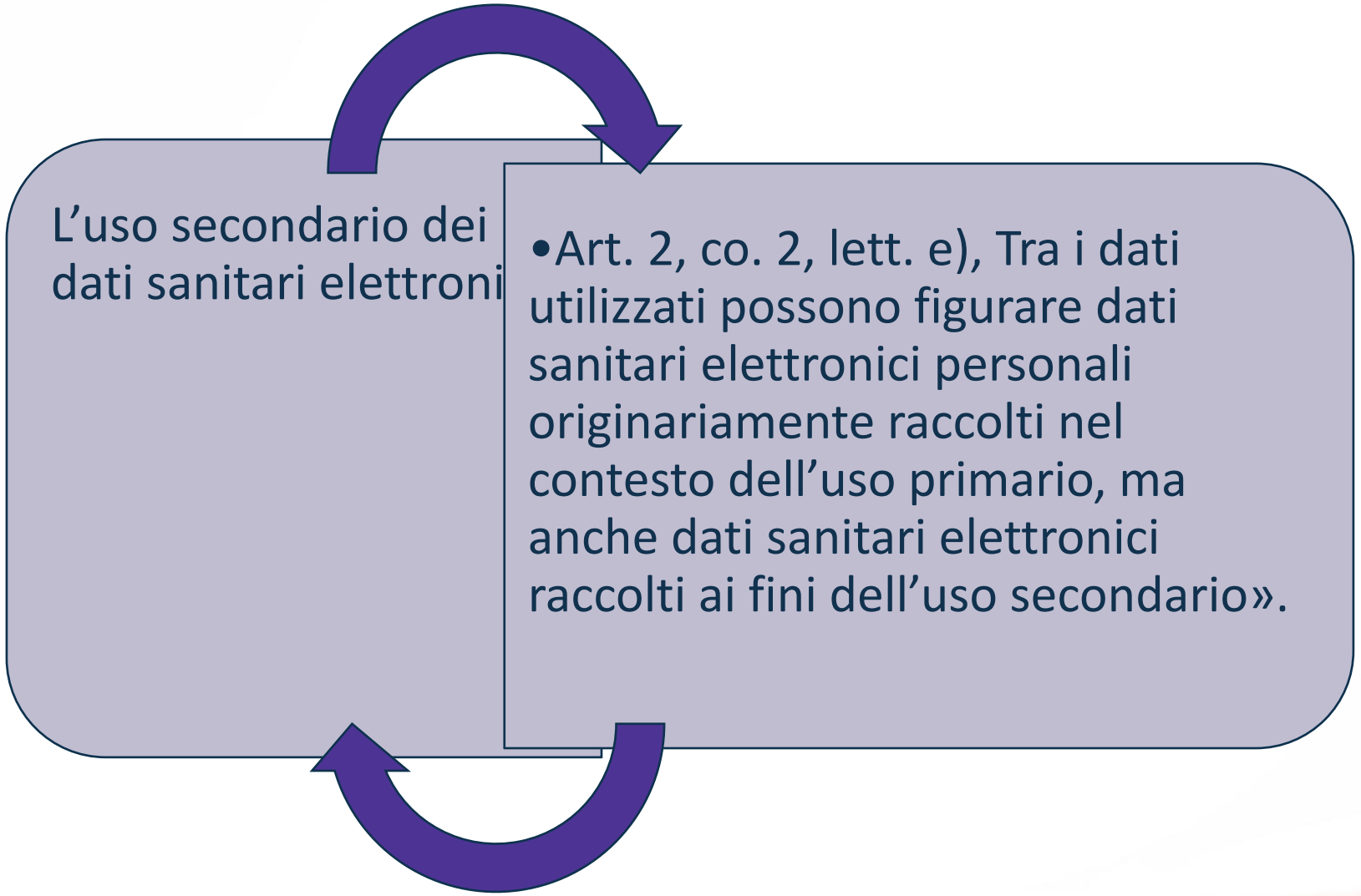
Fa leva sulla normativa europea in tema di cybersicurezza

Criteri di sicurezza/interoperabilità per i sistemi di cartella clinica elettronica (EHR) e marcatura CE

Uso Secondario

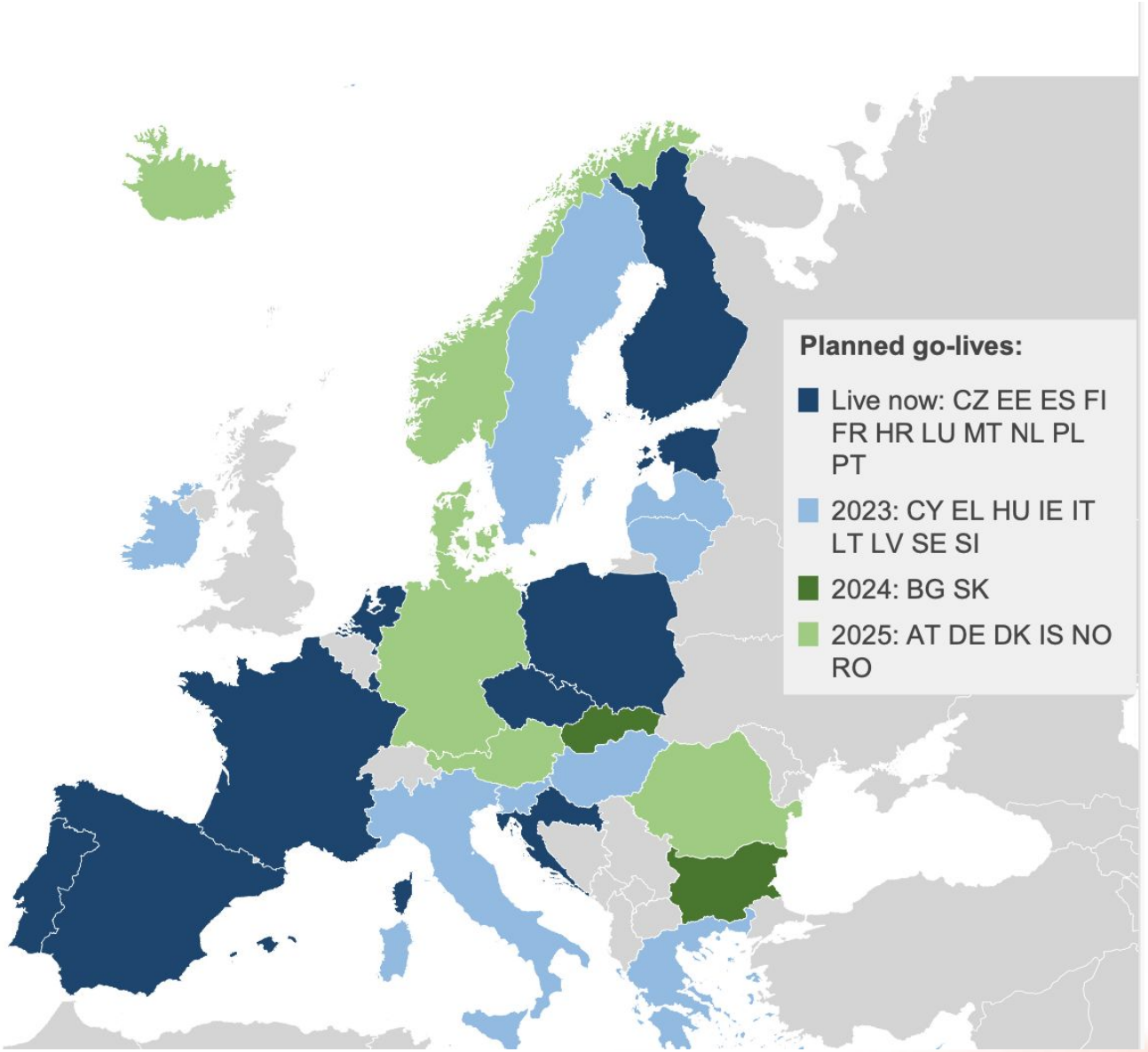


USO Secondario



MyHealth@EU

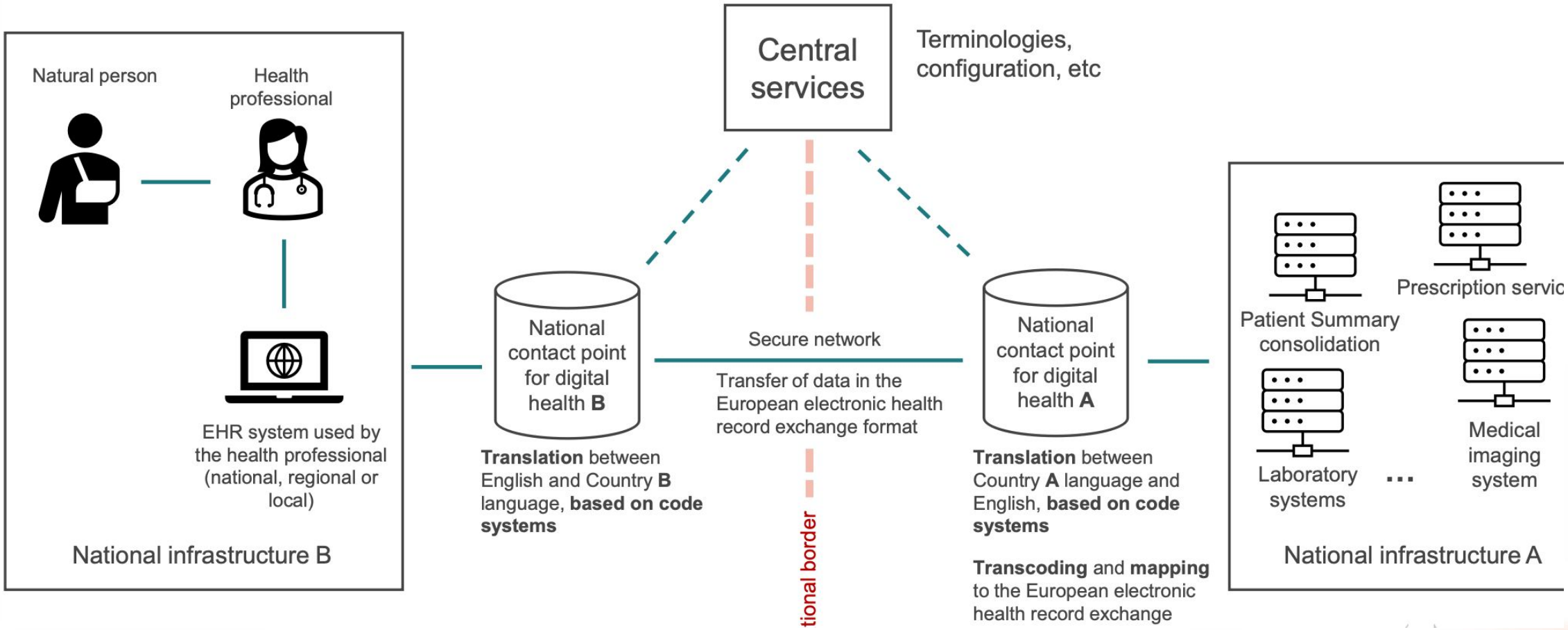
MyHealth@EU is the existing infrastructure that connects healthcare providers in 11 Member States. It allows them to exchange health data such as Patient Summaries and ePrescriptions. These services will be expanded to include lab results and other types of health data.



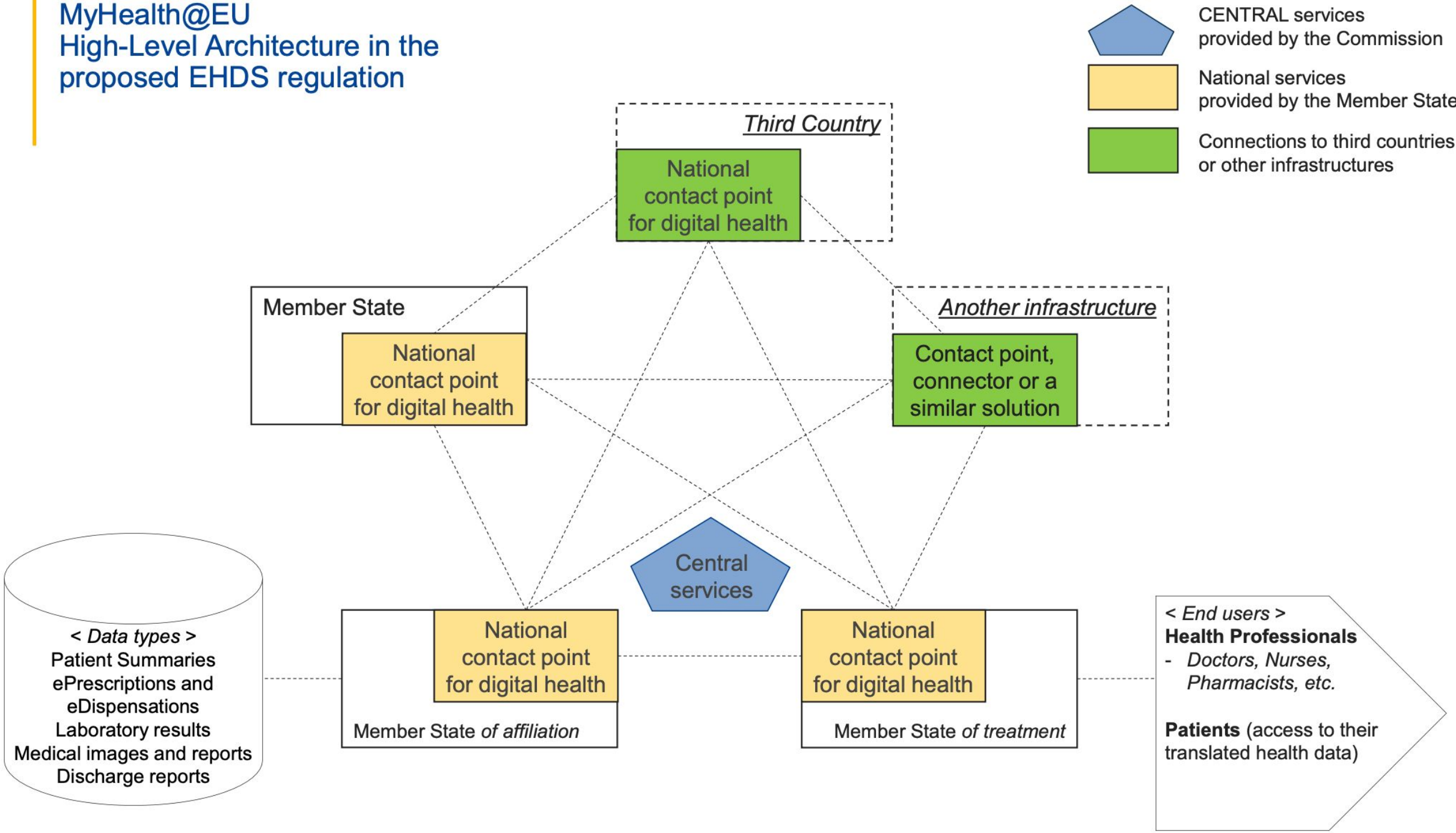
EHDS: Uso secondario

Categorie di dati che i titolari mettono a disposizione per l'uso secondario (art. 33);
Finalità per le quali è possibile trattare I dati sanitari elettronici per uso secondario (art. 34);
Finalità per le quali l'accesso ai dati sanitari ed il relativo trattamento è vietato (art. 35).

MyHealth@EU
Basic data flow in a face-to-face healthcare service



MyHealth@EU
High-Level Architecture in the proposed EHDS regulation



Opt-out

diritto per i cittadini di opporsi alla condivisione dei propri dati per utilizzi secondari

Il i cittadini hanno il diritto di opporsi alla condivisione dei propri dati per finalità di utilizzo secondario

L'accordo introduce un approccio armonizzato all'opt-out:

che impone agli Stati membri di adottare un meccanismo di opt-out accessibile e di facile comprensione.

una volta che un individuo si oppone alla condivisione dei propri dati sanitari per utilizzi secondari, tali dati non potranno essere resi disponibili né trattati.

il diritto di opt-out può essere superato se un organismo di sanità pubblica, un'istituzione o un ufficio dell'Unione richiede i dati per ricerca scientifica di rilevante interesse pubblico

Rischio di applicazione a geometria variabile

EHDS e GDPR: aspetti di contatto

- articolo 21, paragrafo 4: i**l diritto di opposizione deve essere esplicitamente portato all'attenzione dell'interessato e presentato in modo chiaro e separato** da qualsiasi altra informazione al momento della prima comunicazione con l'interessato.
- L'istituto dell'opt-out è disciplinato in modo diverso all'interno dei sistemi giuridici degli ordinamenti nazionale: problema del consenso
- Comitato europeo per la protezione dei dati (EDPB): nei casi in cui il consenso non sia la base giuridica per il trattamento dei dati personali, esso può comunque essere utilizzato come garanzia per il trattamento.

Pseudonimizzazione, anonimizzazione e opt-out: tra compliance e ambiguità

I dati – prima di confluire negli Health Data Access Bodies (HDAB) per essere elaborati – dovrebbero essere pseudonimizzati dai titolari

La responsabilità ultima della piena conformità rimane in capo agli HDAB e che devono assicurarsi che le procedure messe in atto siano effettivamente sicure (FAQ, Q45). Non esiste però un modello unico di pseudonimizzazione (tokenizzazione, hashing, ecc.).

Le FAQ : se un titolare non è in grado di collegare un set di dati pseudonimizzati a uno specifico individuo – per mancanza di identificatori – diventa impossibile onorare quell'opt-out.

Infrastrutture transfrontaliere, tra sicurezza e complessità

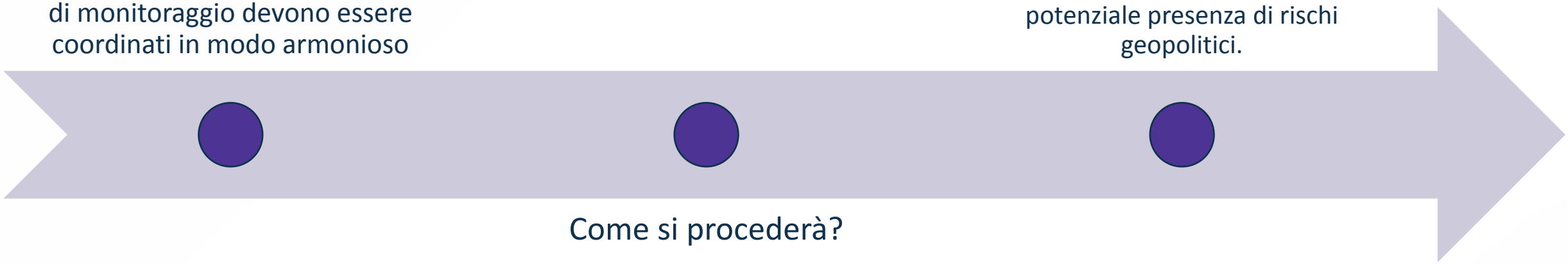
MyHealth@EU (dedicata all'uso primario dei dati) e **HealthData@EU** (pensata per l'uso secondario) richiedono un'attenzione specifica per garantire sicurezza e affidabilità in un contesto sovranazionale.

Uno dei punti di forza di MyHealth@EU è la sua **architettura decentralizzata point-to-point**, priva di un deposito centralizzato. Questo approccio **dovrebbe ridurre il rischio di "mega-data breach"** ma, al contempo, implica che **ciascun nodo nazionale – e quindi ogni Stato membro connesso – adotti standard di sicurezza simili**.

Aspetti di problematicità

Elementi
come **firewall**, **crittografia** e sistemi di monitoraggio devono essere coordinati in modo armonioso

la connessione di Paesi terzi, possibile previa verifica di "equivalenza" nel livello di protezione dei dati. La mancanza di specifiche tecniche dettagliate (ad esempio su protocolli di crittografia end-to-end) potrebbe generare vulnerabilità o "anelli deboli" all'interno della rete (FAQ, Q52), specialmente se si considera la potenziale presenza di rischi geopolitici.



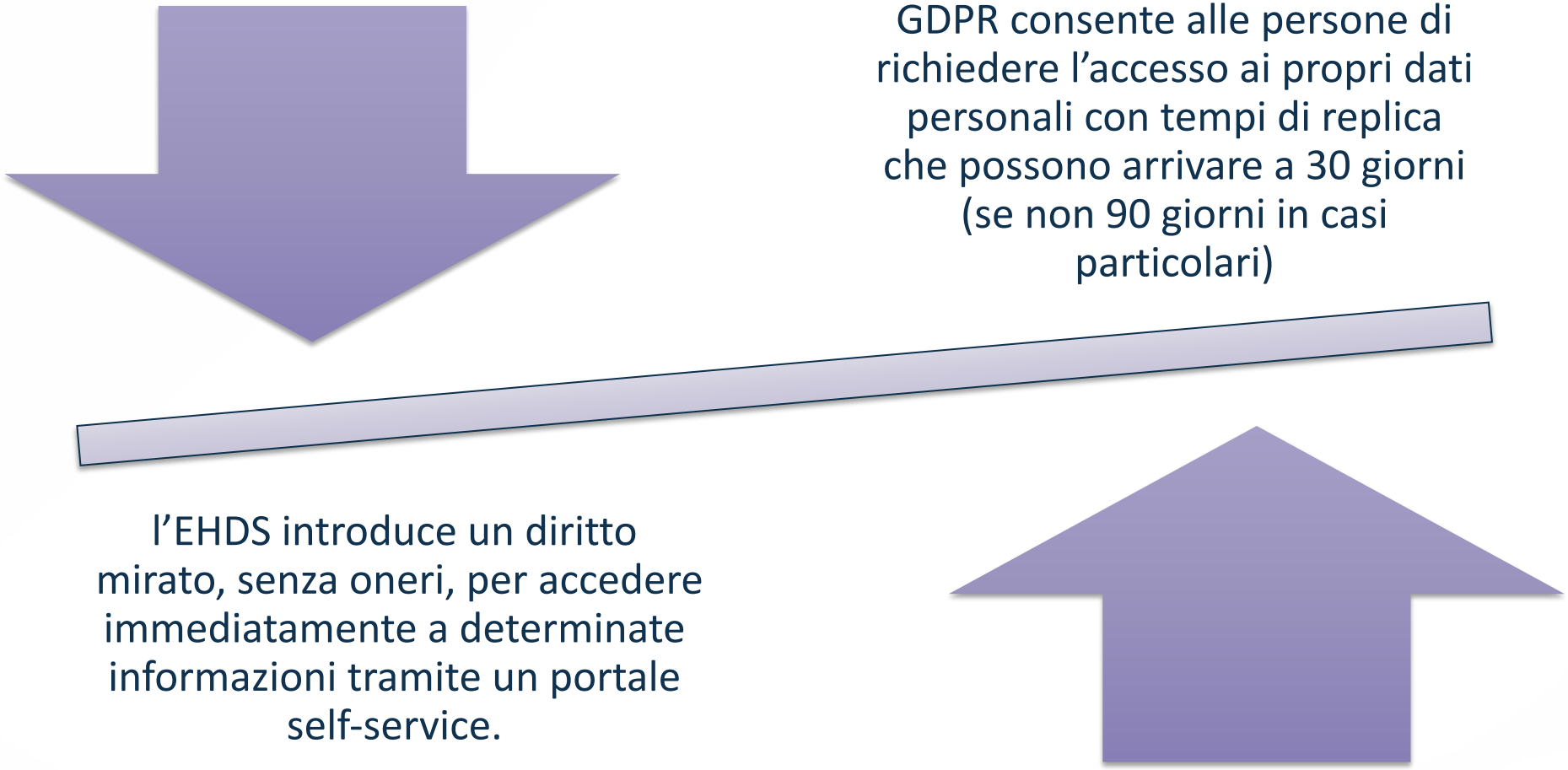
Come si procederà?

HealthData@EU

Secure Processing Environment (SPE), ambienti protetti dove i dataset possono essere analizzati

- i requisiti per garantire un isolamento solido e un controllo degli accessi continuo non appaiono ancora ben definiti nelle FAQ (FAQ, Q73), se questi ambienti venissero compromessi, il danno potrebbe risultare ingente, perché includerebbe dati sanitari di grande rilevanza.
- La piattaforma prevede un **catalogo federato di dataset** gestito dagli Health Data Access Bodies, condivisione che presuppone API sicure e rigorosi sistemi di autenticazione.
- Le FAQ citano generiche “misure tecniche”, senza fornire linee guida precise (FAQ, Q75), lasciando spazio a possibili disomogeneità nelle implementazioni.

EHDS e GDPR: diritti ampliati e responsabilità condivise



GDPR consente alle persone di richiedere l'accesso ai propri dati personali con tempi di replica che possono arrivare a 30 giorni (se non 90 giorni in casi particolari)

l'EHDS introduce un diritto mirato, senza oneri, per accedere immediatamente a determinate informazioni tramite un portale self-service.

Impatto sui progetti di ricerca

European Genomic Data Infrastructure

Secure cross-border access to genomic and health data,
for research, personalised healthcare and public health policy

2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027

Design & Testing

1+MG Declaration

European Commission
Horizon 2020
European Union funding
for Research & Innovation

B1MG Beyond one Million Genomes

EDIC, healthcare uptake

B1MGplus (CSA)

Scale-up & Sustainability

European Genomic Data Infrastructure

The European "1+Million Genomes" (1+MG) initiative facilitates signatory countries to realise a practice of personalised medicine and health, based upon a shared 'framework' and the infrastructure to safely access and integrate high quality genomic data and other health data across borders.

[1+MG Roadmap 2023-2027]

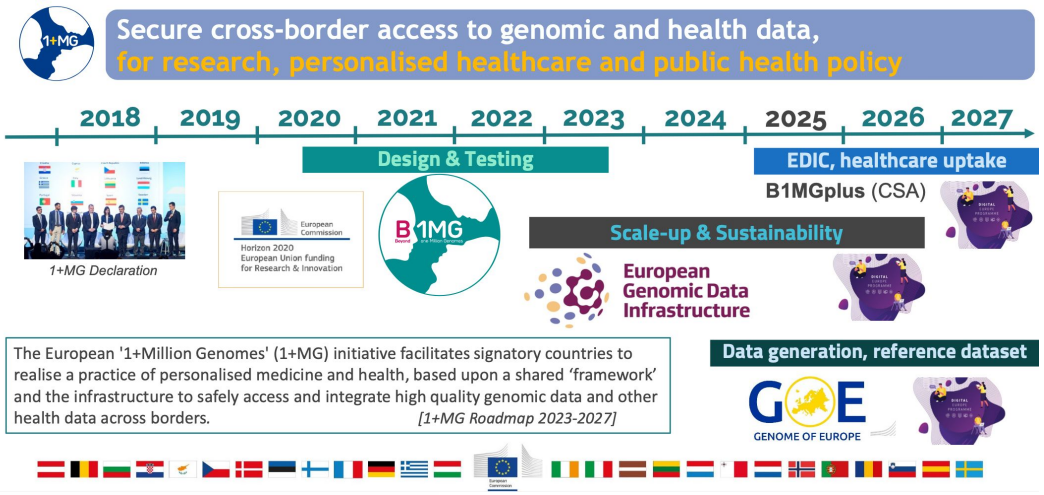
GDI

Data generation, reference datasets

GENOME OF EUROPE

European Commission

European Genomic Data Infrastructure



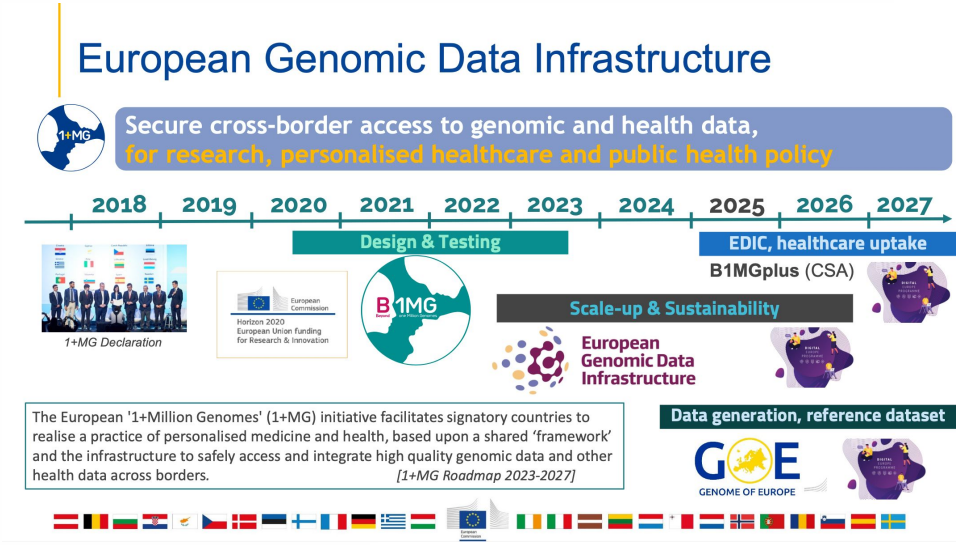
Governance e legge applicabile

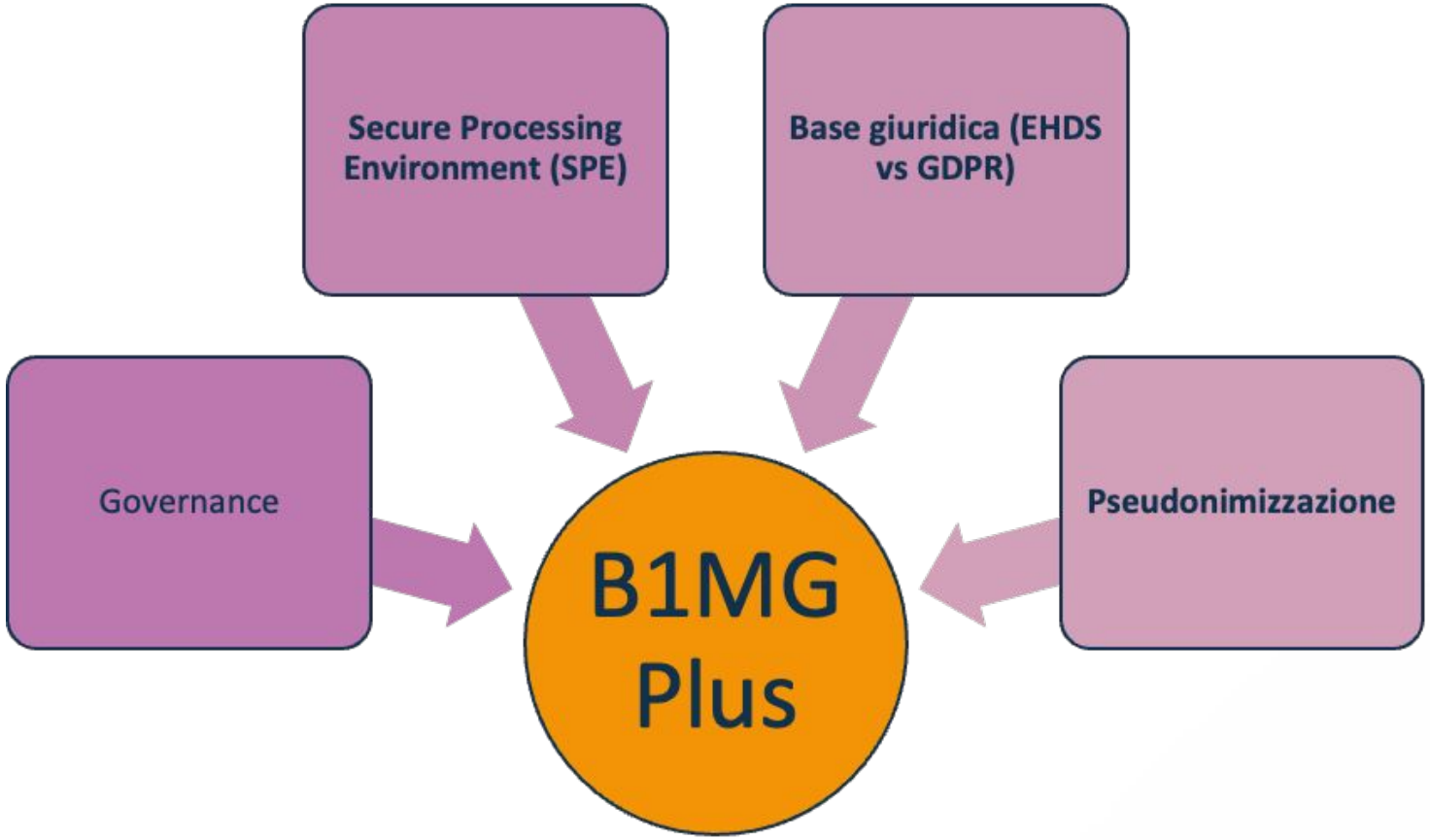
Applicazione EHDS

GDI

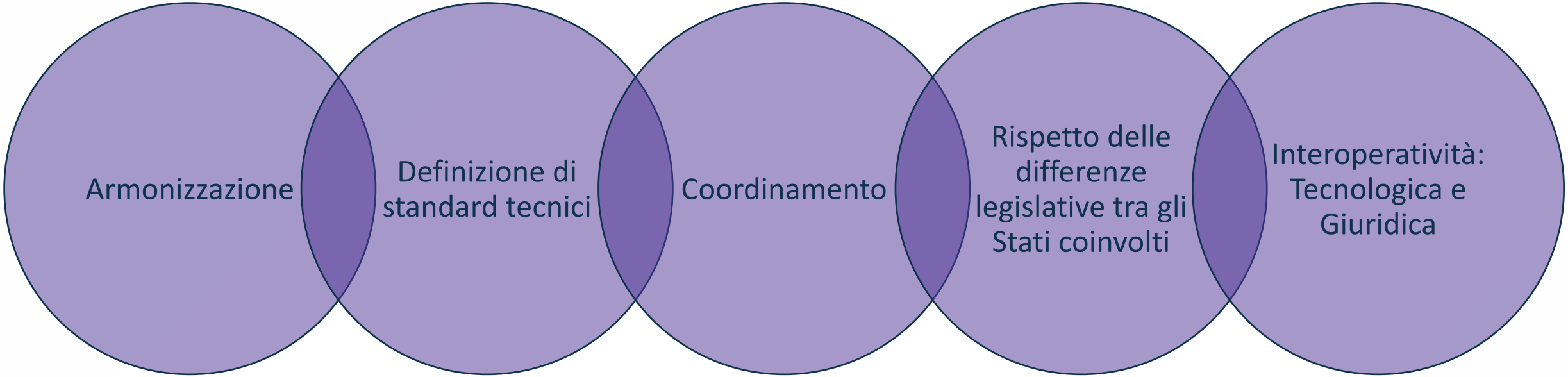
Ruolo di Elixir

Criticità implementative





Conclusioni



Autori:

N. Foggetti, G. Pesole, F. De Leo, B. Fosso, M. A. Tangaro, A. Cestaro, F. Licciulli, C. Lo Giudice, M. Chiara, G. Cauli, M. D'ambrosio

Grazie per l'attenzione

nadina.foggetti@cnr.it
n.foggetti@uniba.it