UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Data Protection: GDPR vs MDR

Ambra Paniccià
BiMind
ambrapaniccia@gmail.com

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Medical Device Regulation (Regolamento EU 745/2017)

«dispositivo medico»: qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche:

— diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie,

— diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità,

— studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico,

— fornire informazioni attraverso l'esame *in vitro* di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati,

e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi.

Si considerano dispositivi medici anche i seguenti prodotti:

— dispositivi per il controllo del concepimento o il supporto al concepimento,

— i prodotti specificamente destinati alla pulizia, disinfezione o sterilizzazione dei dispositivi di cui all'articolo 1, paragrafo 4, e di quelli di cui al primo comma del presente punto;

MDR

Valutazione Clinica

Dati Clinici

L’MDR incrocia il GDPR

Aree del MDR che possono essere di interesse per il GDPR:

- Requisiti di sicurezza e prestazione
- Studi sui dati clinici
- Post-market surveillance e post market clinical follow up
- Maggiore trasparenza (EUDAMED)

I volumi di segnalazione aumenteranno e così anche il volume di dati.
La sfida è rappresentata dalla protezione dei dati personali.

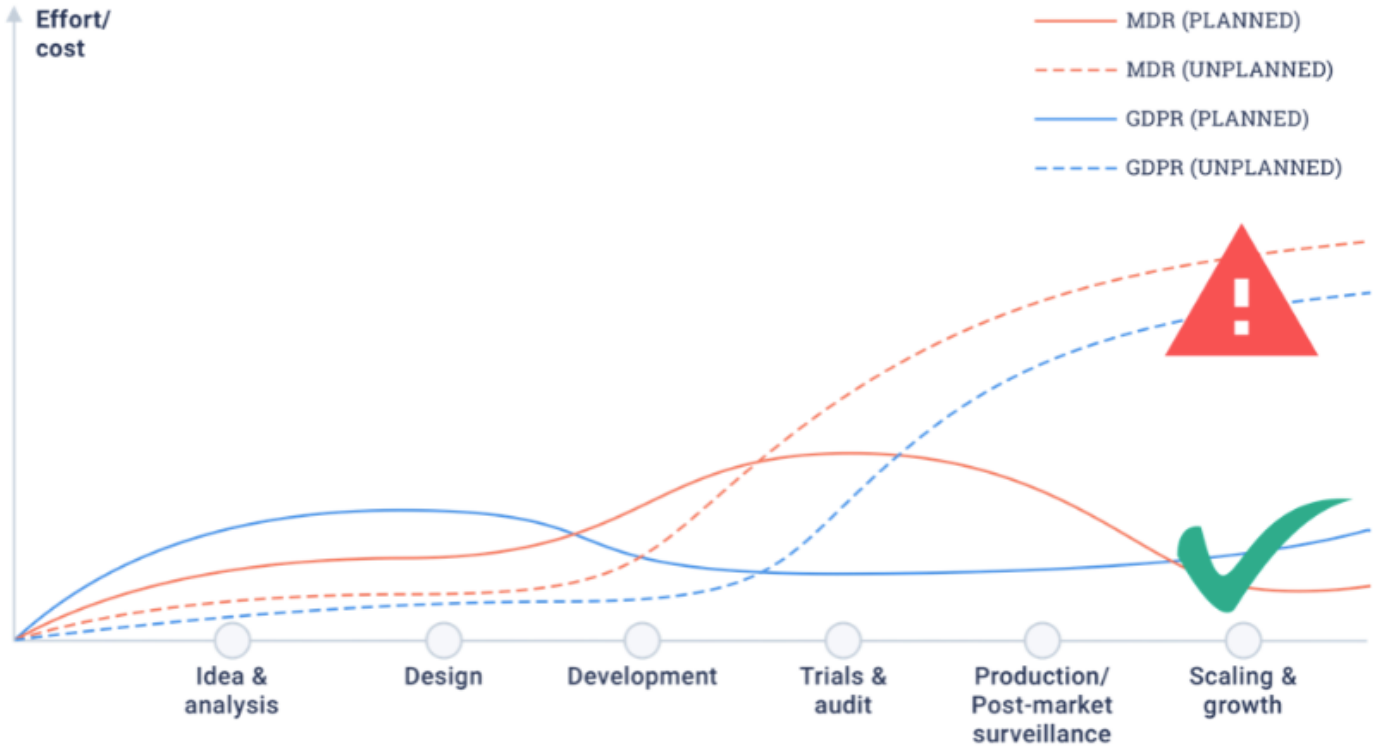
Diritti e libertà fondamentali per la protezione dei dati personali

La raccolta ed elaborazione dati per valutazione clinica, eventi avversi, sicurezza e vigilanza, e post-market surveillance deve essere fatta osservando i principi del GDPR

Determinare policy e procedure per:

- Consapevolezza dei requisiti normativi, dei dati raccolti, dei diritti degli interessati e delle responsabilità
- Utilizzo dei dati per il solo scopo per cui sono stati raccolti
- Implementazione di standard per la protezione dei dati
- Assicurare che le procedure siano aggiornate per riflettere i requisiti GDPR e rilevare le violazioni
- Training sui requisiti del GDPR a tutto il personale che gestisce dati personali

GDPR E MDR BY DEFAULT

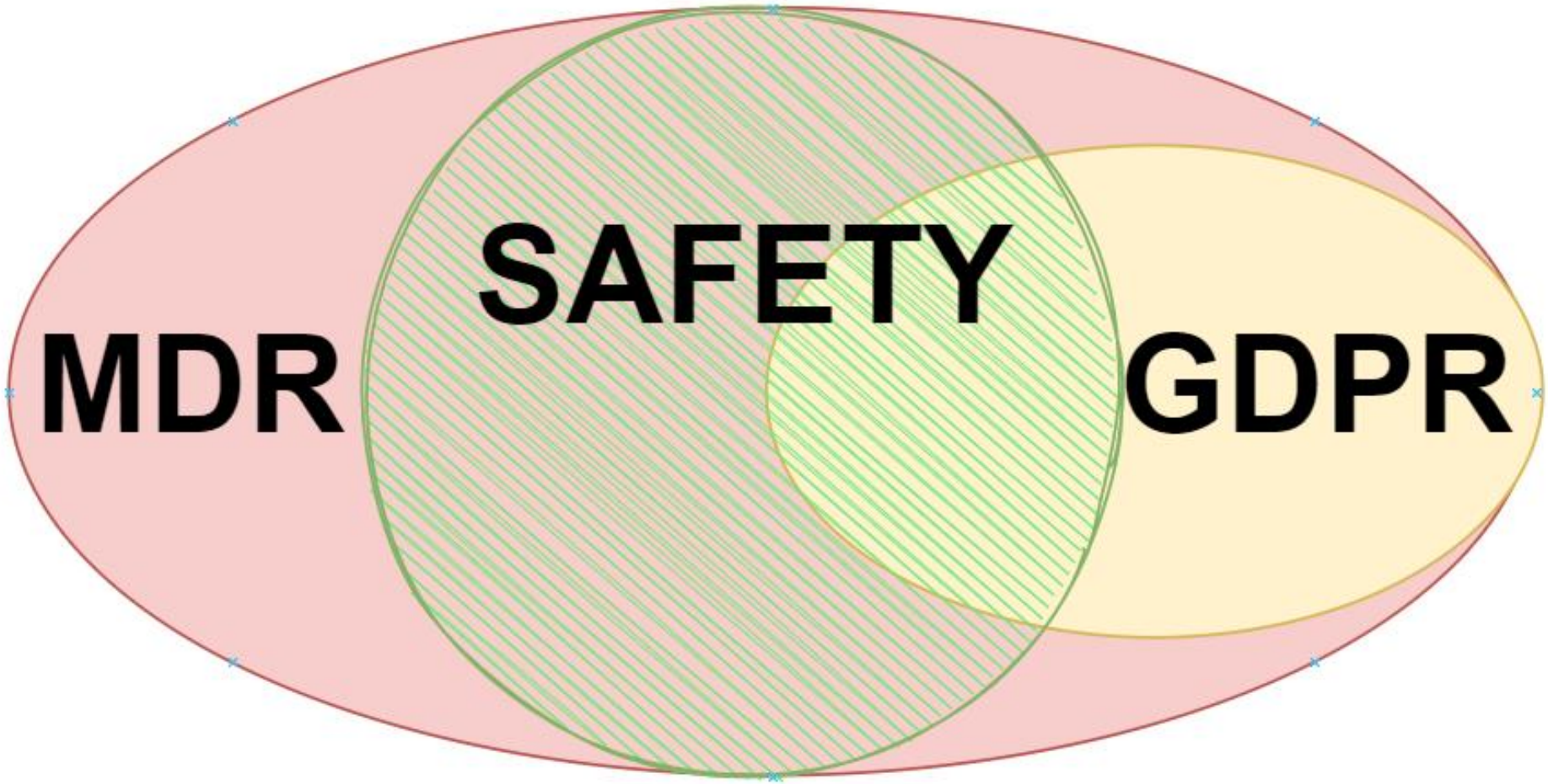


MDR	Understand what MDR category you fall in. Get ISO13485.	Choose suppliers and complete ISO 13485 requirements.	Document the development process.	(Class IIa +) Perform trials. Document results.	Surveillance and monitoring of application.	Ongoing change tracking and documentation
GDPR	Identify data you are going to collect. Identify your requirements.	Consider security, privacy, and compliance requirements.	Add tools to enable user consent tracking, etc.	Ensure data security.	Data security. Consent tracking. Right to be forgotten.	Scale backend.

Far coincidere le misure tecniche e organizzative per ridurre i rischi di safety e di security.

Considerare la compliance a GDPR e MDR by default. L'adeguamento delle misure tecniche e organizzative per la conformità richiede tempo, fatica e costi.

GDPR E MDR



GDPR

R iservatezza

I ntegrità

D isponibilità

R esilienza

Pericolo **SAFETY**

Conclusioni

Elevata complessità che richiede conoscenze e competenze molto ampie a livello normativo e tecnologico.