Every time you visit a doctor, fill in a prescription, or use a health app, information about you is being collected, stored, and shared. Who is responsible for protecting it? Who is allowed to see it? And what rights do you actually have over it?

SAFEPOLYMED

SafePolyMed.eu

Improving Safety in Polymedication by Managing Drug-Drug-Gene Interactions

Safety in Polypharmacy training 2026

Session 7 - Video 1/3

Data Safety, Privacy, and GDPR

GDPR Fundamentals: Understanding Your Data Rights

Patricia Cervera de la Cruz, Dominique Hamerlijnck, Joan Jordan, Olga Millán

LeukaNET Leukemia Advocates Network

Patvocates PATIENT ENGAGEMENT IS IN OUR DNA

Funded by the European Union

AI Disclosure: *Avatars, voices, and some visual elements in this video were generated using HeyGen & Copilot. The educational content was created by humans and subsequently edited and summarised with AI assistance.*

What Counts as “Personal Data”?

Personal data is any information relating to an identified or identifiable person, a "**data subject**"



Data Subject



Name / ID number



Location data



Genetic traits



Social Identity

Processing

Any operation on that data, automated or not:

- *Collection*
- *Recording*
- *Storage*
- *Adaptation*
- *Retrieval*
- *Consultation*
- *Combination*
- *Restriction*
- *Disclosure*
- *Erasure*

https://gdpr-info.eu/art-4-gdpr/

Who is Responsible? Controller vs. Processor

The **controller** decides why and how personal data is used.

The **processor** handles that data on the controller's behalf, following instructions.



https://gdpr-info.eu/art-4-gdpr/
https://gdpr-info.eu/art-6-gdpr/

The Right to Data Protection and What the GDPR is

Article 8 of the EU Charter of Fundamental Rights. Protection of personal data

EU Charter of Fundamental Rights Article 8

- Data must be processed fairly, for specified purposes
- Based on consent or another legitimate legal basis
- Right to access and correct your own data
- Compliance overseen by an independent authority

GDPR - General Data Protection Regulation

The comprehensive law that puts this right into practice, governing how personal data of individuals in the EU is collected, processed, and stored.

99 Articles | 173 Recitals



It applies to any company doing business in the EU, and to all personal data belonging to EU citizens or residents. People outside the EU can fall under the GDPR's protection too.

https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data
https://gdpr-info.eu/

Free Movement of Data Within the EEA

Core GDPR principle: The free movement of personal data cannot be restricted for data-protection reasons, but only within the European Economic Area - EEA (EU + Iceland, Liechtenstein, Norway).

Countries outside the EU or EEA don't automatically benefit from this free flow of data.

Free flow within the EEA

Controller in the Czech Republic → cloud provider in Norway.
Both are within the EEA, so no additional legal basis needed.

Needs an additional legal basis

Controller in Spain → provider in Switzerland.
Provider outside the EEA, so an adequacy decision or other legal basis is required.

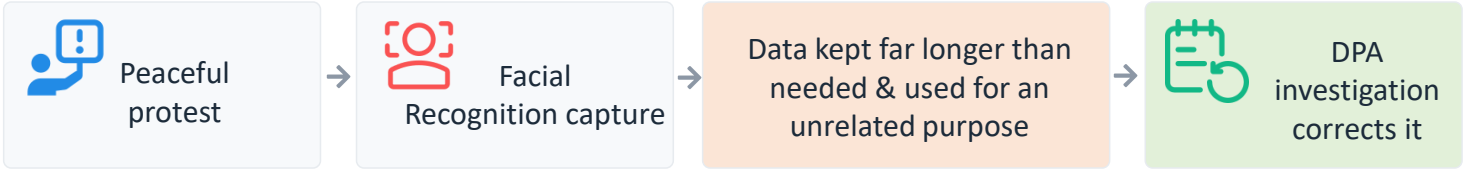
https://www.planetcompliance.com/gdpr-challenges-opportunity/
https://gdprhub.eu/Article_1_GDPR#:~:text=Under%20Article%201(3)%20GDPR,so%2Dcalled%20data%20localization%20laws.

The Seven Principles of GDPR

- Lawfulness, fairness & transparency
- **Purpose limitation**
- **Data minimisation**
- Accuracy
- Storage limitation
- Integrity & confidentiality
- Accountability

Personal data must be collected only for a specified purpose, and it cannot later be reused for a different, incompatible purpose.

A real scenario:



Recommended video: https://youtube.com/playlist?list=PLgrQeHXIMX5MnDeWBDPLzHfYhIm7rM-0n&si=cn7ZEpv7HNv0QyCr

https://gdpr-info.eu/chapter-2/

Legal vs. Ethical Approaches to Data Protection



Legal Approach

Rule-based, objective, enforceable. Focused on compliance with established laws and avoiding penalties.



Ethical Approach

Fairness, transparency, and consent as an ongoing process, balancing innovation with privacy.

Dhirani, L. L., et al., (2023). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. Sensors, 23(3), 1151.
https://doi.org/10.3390/s23031151
https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

Who Enforces the GDPR?



European Data Protection Board (EDPB)

European Data Protection Board. Consistent application, binding cross-border decisions





National Data Protection Authorities (DPAs)

Each EEA country's independent authority. Oversees compliance, investigates complaints, cooperates across borders



European Data Protection Supervisor (EDPS)

Independent authority monitoring EU institutions themselves and providing formal guidance.

Recommended video: https://youtu.be/NtoECH1Kq54

https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en
https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en
https://www.edps.europa.eu/about-edps_en

Applying GDPR to New Technologies

Despite the fast-moving technologies, GDPR principles still apply. The EDPS actively guides how it should be interpreted.

Artificial Intelligence in Healthcare

- Systems that analyse records or predict outcomes must still follow data minimisation & purpose limitation
- Patients keep a right to explanation for automated decisions made about them
- Developers & providers share responsibility for privacy-safe design

Neurodata & Neurotechnology

- Devices that read brain activity for pain relief, gaming, or mental health generate highly sensitive data
- This "neurodata" carries real privacy risk if mishandled
- EDPS calls for stronger consent processes and dedicated safeguards

https://www.edpb.europa.eu/system/files/documents/2024-12/edpb_opinion_202428_ai-models_en.pdf
https://www.edpb.europa.eu/topics/ai-and-technology/artificial-intelligence_en
https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata_en

SAFEPOLYMED

Key Takeaways

Understanding what personal data is, who is responsible for it, and how the GDPR protects it sets the stage for everything else in this session.

- Personal data & processing
- Controllers vs. processors
- The right to data protection
- GDPR's seven principles
- Who enforces it

Coming up next: **Video 2 — GDPR in Health Research & Polypharmacy**

SAFEPOLYMED

Credits & Attributions

Authors

Patricia Cervera de la Cruz | Dominique Hamerlijnck | Joan Jordan | Olga Millán

AI disclosure

Avatars, voices, and some visual elements in this video were generated using HeyGen & Copilot. The educational content was created by humans and subsequently edited and summarised with AI assistance.

Icons

- Selected icons adapted from Font Awesome Free by Fonticons, Inc. - fontawesome.com – licensed under CC BY 4.0. Colours modified.
- Selected icons by Icons8 - http://icons8.com/icons