

## Federated Learning, Privacy, and Regulatory Challenges

Federated Learning (FL) represents a promising approach for enabling large-scale biomedical research while preserving data privacy. By allowing models to be trained locally on decentralized data, FL aligns well with data minimisation and confidentiality principles outlined in the General Data Protection Regulation (GDPR). However, despite its advantages, FL introduces complex policy and regulatory challenges that must be addressed to ensure responsible, large-scale adoption—particularly in sensitive domains such as health and biomedical research.



### Legal responsibility and accountability

- Who is considered the data controller or processor in a federated learning setup?
- How should liability be distributed when multiple institutions collaborate in an FL environment?
- What contractual or governance mechanisms are required to define roles and ensure compliance?



### Data protection and privacy metrics

- Current PETs (Privacy-Enhancing Technologies) offer mitigation, but lack of reliable privacy metrics can lead to blind spots in risk evaluation.
- There is a need for standardized tools and methods to quantify privacy leakage and guide data-sharing decisions in real time.
- While FL helps minimize data sharing by design, incorporating PETs is essential to ensure stronger privacy guarantees during training.



### Alignment with GDPR principles

- While FL supports data minimisation and local control, uncertainty remains about the sufficiency of existing PETs in meeting GDPR's expectations around data protection by design and by default.
- Policies must clarify how FL frameworks can demonstrate compliance in a legally defensible way.

## OPEN QUESTIONS

- 1 How can **secondary use of health data** through FL infrastructures comply with GDPR?
- 2 Can **regulatory sandboxes** or pilot frameworks help test and validate FL technologies under real-world constraints?
- 3 What mechanisms can be used to **audit or certify FL implementations** for privacy compliance?
- 4 How can **transparency be ensured** without exposing sensitive architecture or training dynamics?

## TRUMPET contribution

- Developed **new theoretical privacy metrics** to assess privacy leakage in FL.
- TRUMPET metrics are **grounded in real-world inference attacks** and aligned with IEEE standards and ENISA recommendations
- Created a **regulatory roadmap** to support broader adoption of FL in biomedical contexts.
- Provided policy-relevant evidence on how **PETs can mitigate risks and support GDPR compliance**.
- Evaluated the practical application of several complementary PETs tailored for Federated Learning.