LeakPro: Unlocking AI Innovation requires Privacy Risk Assessment

Your AI models may leak personal data or trade secrets. GDPR and the AI Act now expect you to prove they don’t. We deliver reproducible, audit-ready assessment of training data leakage — don't wait for unpleasant surprises.

Henrik Forsgren and Rickard Brännvall
RISE – Research Institutes of Sweden

mailto poster

Does your AI remember things it shouldn’t?

AI can only scale if people trust it. Leaks of medical data, images or proprietary information undermine that trust — and regulators are tightening expectations. Even government agencies struggle to share data or models when there’s a risk of hidden memorisation. Reducing that uncertainty is key to unlocking safe, lawful and commercially viable AI development.

IMY Sandbox on AI model sharing

Sweden’s first regulatory testbed identified leakage risks in federated learning and cross-provider collaboration, underscoring the need for controlled environme4nts where AI can be evaluated before deployment — a need now reinforced at EU level, where the AI Act requires every member state to operate a sandbox for testing AI systems prior to use.

eSam’s position on AI Regulatory Sandboxes

The government-agency collaboration program for digitalisation, eSam, calls for a national capability for AI evaluation, emphasising the need for practical verification methods to show that privacy protections actually work.

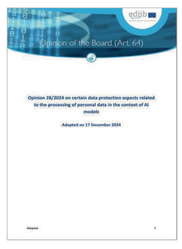
Use case:	*Principal:*
Hospital length of stay	Health care provider
	Data modality:
	Tabular data (EHR)
	Risk factors:
	Re-identification
	Attribute inference

Use case:	*Principal:*
Camera surveillance 	Public authority
	Data modality:
	Facial images
	Risk factors:
	Image reconstruction
	Loss of confidential info

AI Commission’s Roadmap for Sweden

Sweden must deploy AI responsibly and develop methods to prove that AI systems are safe and trustworthy. The roadmap points to challenges around data protection and regulation — and explicitly calls for research into practical PETs that can strengthen privacy in real-world use.

EDPB Opinion on Anonymity of AI Systems



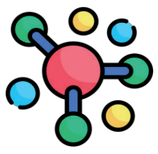
Clarifies that AI models trained on personal data are not automatically anonymous — this must be proven. The risk of extracting personal data must be insignificantly small, supported by documentation and auditable testing methods. The opinion also discuss techniques for assessing identifiability.

Recent EU clarifications — from updated guidance on pseudonymisation to a European Court of Justice ruling on third-party data processing — reinforce a key message: identifiability must be assessed from the receiver’s perspective and judged against the means realistically available.

IMY Sandbox on Synthetic Data

Synthetic data can support data protection, but it is not automatically anonymous – it still requires leakage testing before use.

Use case:	*Principal:*
Text-masking 	Government agency
	Data modality:
	Text documents
	Risk factors:
	Re-identification
	Named-entity prediction

Use case:	*Principal:*
Molecule properties 	Pharmaceutical company
	Data modality:
	Proprietary graph data
	Risk factors:
	Molecule feature prediction
	Loss of valuable IP

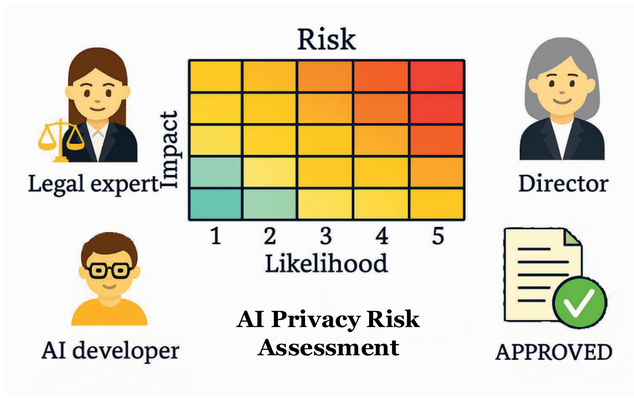
Our example portfolio of real industry use cases cover four distinct data modalities: tabular, image, text, and graphs. The privacy risk factors correpond to different attacks against the data.

The privacy triagle illustrates three perspectives on privacy risk that can be difficult to reconcile.

Government Inquiry – PETs in the Public Sector

Recognises the need for privacy-preserving methods to enable data sharing between goverment authorities, calls for expertise and national capability, and signals potential future legal developments to strengthen the use of PETs.

Across Europe, a clear message is emerging: privacy risks must be demonstrated, not assumed. Regulators accept that risk can never be zero, but expect quantitative, auditable evidence to show that identifiability is reduced to an insignificant level. This marks the transition to measurable privacy risk assurance.



HOW WE CAN HELP

Privacy testing. Asses risk for AI models and synthetic datasets for information leakage – prepare evidence for regulatory reporting (DPIA).

RISE Research Institutes of Sweden
www.ri.se / info@ri.se

CONTACT
Henrik Forsgren, henrik.forsgren@ri.se