From Promise to Practice

Overcoming the Barriers to PET Adoption

Dr. Alexandra Klymenko, CIPM

12 October 2026 · Munich



Privacy-Enhancing Technologies (PETs) have been at the center of my work for almost seven years

About me

Originally from **Ukraine**, **10 years** in Germany

PhD: Supporting the Informed Adoption of Privacy-Enhancing Technologies
Computer Science, Technical University of Munich (TUM)

>6 years of research on PETs, continuing privacy research as a **Guest Researcher at TUM**

Senior Consultant, Digital Trust & Security team at **Capgemini Invent**



alexandra.klymenko@capgemini.com / @tum.de
linkedin.com/in/alexandra-klymenko

Today we will explore what PETs are and what value they can bring

(Concise) agenda

01 What are Privacy-Enhancing Technologies (PETs)?

02 Why are they needed and what value can they bring to organizations?

03 Why is adoption lagging and what can we do as a community to change this?

+ Bonus: PETs and AI

PETs represent a class of “technical measures” that can help achieve privacy compliance and data protection

The motivation for this work

Regulatory compliance

The mandate

- GDPR requires implementing “appropriate technical measures”
- Compliance is often the primary driver of privacy efforts

Technical measures / PETs

The means

- PETs help to address the technical side of compliance
- Yet they are rarely adopted in practice

Adoption gap

Beyond compliance

The motivation

- Laws don’t explicitly require advanced PETs
- Incentives to go beyond the “bare minimum” are lacking

Roles that shape the decision

Management

e.g., CISO, CTO, privacy manager

Development

e.g., software engineers, software architects

Legal

e.g., privacy lawyers, compliance officers

“Go-betweens”

e.g., DPO, privacy engineer

Our research investigated how to support PET adoption from management, technical, and legal perspectives.

Source: Klymenko, O. et al.: *Understanding the Implementation of Technical Measures in the Process of Data Privacy Compliance: A Qualitative Study.* In: 16th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), 2022

Both academia and industry show little consensus on how to define PETs and which technologies fall under the term

The definition of PETs

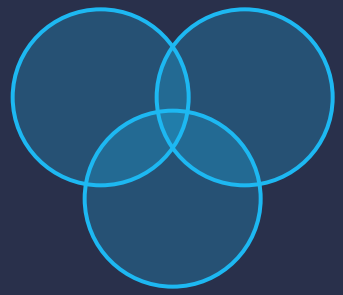
1995

PETs first mentioned

Academia

No unified definition

Different works classify different technologies as PETs



Industry

The term is rarely used

The term is often misunderstood or not used at all by practitioners



A common definition creates demand for PETs and gives practitioners a reference to act on.

Source: Klymenko, A. et al.: *"Do We Call Them That? Absolutely Not.": Juxtaposing the Academic and Practical Understanding of Privacy-Enhancing Technologies.* In: Symposium on Usable Security and Privacy (USEC), 2025

We developed a unified definition of PETs through a review of 37 academic surveys on PETs and input from 80+ privacy experts

The unified definition of PETs

Privacy-Enhancing Technologies (PETs) are a collection of **technical measures** to **protect the rights and freedom of data subjects** by **eliminating, altering, or minimizing the processing of their personal data**.

These technologies, when properly implemented, can **prevent direct or indirect linkage** between data subjects and their data, while allowing processing entities to **derive value from data** in a way that is **compliant** with applicable data protection regulations.

Technical measures
What PETs are and do

Protect data subjects
What PETs safeguard

Value and compliance
What organizations get

In this work, we consider advanced PETs such as Differential Privacy (DP) or Homomorphic Encryption (HE).

Source: Klymenko, A. et al.: *"Do We Call Them That? Absolutely Not.": Juxtaposing the Academic and Practical Understanding of Privacy-Enhancing Technologies.* In: Symposium on Usable Security and Privacy (USEC), 2025

Understanding the main PETs and their real-life use cases helps identify where they fit in your organization

The 5 PETs worth knowing

PET	Differential Privacy	Homomorphic Encryption	Secure Multi-Party Computation	Federated Learning	Zero-Knowledge Proofs
Definition	Adds calibrated statistical noise so individual records can't be re-identified, while aggregate insights stay accurate.	Enables computation directly on encrypted data, producing results that decrypt to the same answer as on plaintext.	Multiple parties jointly compute a function over their combined inputs while keeping each input private from the others.	Trains ML models across decentralized devices without moving raw data to a central server.	Lets one party prove a statement is true without revealing any of the underlying information.
In real life	The US Census shares statistics without exposing individuals.	A cloud service analyzes locked patient data without ever seeing it.	Colleagues work out their average salary without anyone revealing their own pay.	Your phone keyboard learns your typing style and only sends back model updates, not your messages.	Prove you are over 18 without showing your birth date or name.

Despite their promise and potential, state-of-the-art PETs remain largely in academia and are not often adopted in practice

Challenges in implementing PETs (and general technical privacy measures)

01 Tech-legal divide

Communication
- Rare interaction
- Poor-quality interaction
- Mindset deadlock

Knowledge and set-up
- Little domain knowledge
- No technical input
- No cross-functional teams

Interpretation
- Interpreting regulations
- Gap seen as desirable

02 Technologies

Understanding
- PETs poorly characterized
- Hard to communicate
- Little education on PETs
- Low technical literacy
- Unaware of existing tools

Practicality
- High resource demands
- No technical framework
- No mapping to regulations

Motivation
- No incentives to adopt
- Privacy-innovation tension

03 Organizational factors

Leadership and culture
- Depends on management
- Depends on culture
- No uniform roles

Support
- Little privacy engineering
- Uneven legal support

Decision-making
- The “it depends” problem
- Seen as a financial cost
- Tied to risk assessment

04 General

Regulation
- Many rules and settings
- Bureaucracy
- Industrialized compliance
- Unequal compliance

The concept of privacy
- Unclear what privacy is
- Confused with security
- Meaning of privacy lost

Source: Klymenko, A. et al.: *Identifying Practical Challenges in the Implementation of Technical Measures for Data Privacy Compliance.* In: 29th Americas Conference on Information Systems (AMCIS), 2023

Overcoming the barriers to PET adoption requires making PETs easier to adopt and worth adopting

Solutions to support PET adoption

Reduce complexity & build capability

Privacy tools
Encapsulate complex implementation in usable libraries and interfaces

Educational material
Bridge theory and practice and build technical understanding

Standardization
Provide accepted guidelines, best practices and protocols

Guide selection & assure compliance

Mappings
Link PET properties to real-world use cases and requirements

Certifications
Demonstrate compliance, credibility and professional competence

Authority contribution
Provide guidance, explicit mandates and regulatory enforcement

Strengthen business & market pull

Privacy awareness
Show financial value, reputation benefits and customer trust

Financial incentives
Offset the cost of researching and implementing PETs

Tech leader adoption
Let larger firms demonstrate viability and diffuse adoption to SMEs

Source: Klymenko, A. et al.: *Supporting the Integration of Privacy-Enhancing Technologies into the Software Development Life Cycle.* In: SN Computer Science 6(6), 2025

PET adoption is an interdisciplinary effort that requires coordinated action inside the organization

Stakeholders involved in PET adoption

Internal roles

Focus of our work

Management — Sets priorities, allocates resources and approves investment

Legal teams — Interpret obligations, assess risk and assure compliance

Technical teams — Evaluate, select, integrate and maintain PET solutions

Outcome

PET adoption

Requires all three roles acting together

External influencers

Out of scope

Regulators & authorities

Set rules, guidance and enforcement expectations

End users & customers

Shape trust, expectations and market demand

Other external actors

May also influence the adoption environment

Management Perspective



PET adoption is ultimately a management decision and managers often lack a clear incentive to make it

The management perspective



PET adoption depends not only on technical factors but also on **organizational context** and **leadership decisions**



Whether to use PETs as technical privacy measures is ultimately a **decision made by senior management**



Lack of incentive is among the main reasons many organizations are still reluctant to use modern PETs

- "Obvious" incentive: the demonstration of compliance to avoid fines
- However: data protection laws and regulations do not explicitly require the use of advanced PETs

What might motivate organizations to surpass the bare minimum and invest in advanced PETs?

Source: Klymenko, A. et al.: *Investigating the Motivational Factors Influencing Managerial Decisions to Adopt Privacy-Enhancing Technologies.* In: 32nd European Conference on Information Systems (ECIS), 2024

We identified a direct link between Corporate Social Responsibility and the adoption of PETs

PETs and Corporate Social Responsibility (CSR)

CSR

Acting "**beyond** narrow economic, technical, and legal requirements"*

+

Privacy

A recognized CSR initiative when **law alone is insufficient**

›

PET adoption

A concrete CSR action

Going **beyond** basic legal compliance to protect privacy

Three foundational categories from CSR*

Moral

Doing the right thing

- Personal values
- Sense of social responsibility

Relational

Keeping stakeholders on side

- Trust with stakeholders
- Good products and services

Instrumental

Reaching company goals

- Legal compliance
- Competitive advantage

* Aguilera, R.V. et al.: *Putting the S Back in Corporate Social Responsibility: A Multilevel Theory of Social Change in Organizations.* In: Academy of Management Review 32(3), 2007

Organizations have many more reasons to adopt PETs than compliance alone

Motivational factors for PET adoption, categorized into three CSR-based groups

Incentives

1. Moral

1. Subjective values
- Right to privacy
- Justice & fairness
- Personal interest in privacy
- Privacy as a personal matter

2. Social responsibility
- Avoid harm to customers
- Avoid customer vulnerability
- Respect human rights
- Concern for community & society

2. Relational

1. Trust building with stakeholders
- Accountability for actions
- Transparency on privacy
- Signals care for stakeholders
- Gains stakeholder trust
- Gains stakeholder loyalty
- Gains stakeholder satisfaction
- Secures stakeholder cooperation
- Gains social legitimacy

2. Provision of a good product/service
- Prioritizes customers' privacy needs
- Privacy as differentiator
- Goal: safe product/service
- Privacy as a feature

3. Instrumental

1. Legal & regulatory compliance
- Legal compliance
- Regulatory compliance
- Organizational survival
- Avoid penalties & breaches

2. Competitive advantage
- Differentiation from competitors
- Mimicry behavior
- First-mover advantage
- Privacy/PETs as USP

3. Reputation & brand image
- Perceived privacy leader
- Strengthens reputation
- Demonstrates CSR

4. Risk mitigation
- De-risks the business
- Mitigates breach impact
- Avoids financial harm
- Prevents reputational damage
- Avoids business loss
- Mitigates spillover effects

5. Long-term success
- Talent attraction & retention
- Customer attraction & retention
- Organizational sustainability
- Market-entry requirement
- Long-term efficiency gains

6. Future readiness
- Adapts to changing rules
- Establishes company vision
- Encourages proactive behavior
- Anticipates PET adoption
- Prepares for privacy-aware users

Source: Klymenko, A. et al.: *Investigating the Motivational Factors Influencing Managerial Decisions to Adopt Privacy-Enhancing Technologies.* In: 32nd European Conference on Information Systems (ECIS), 2024

Privacy managers support all three categories of incentives for the adoption of PETs

Results of the survey with 15 privacy managers who adopted PETs

"As a manager / decision-maker, I am motivated to adopt PETs as technical measures for privacy protection because…"

Agreement by incentive category

Moral

86%
agree

59%
strongly agree

Relational

83%
agree

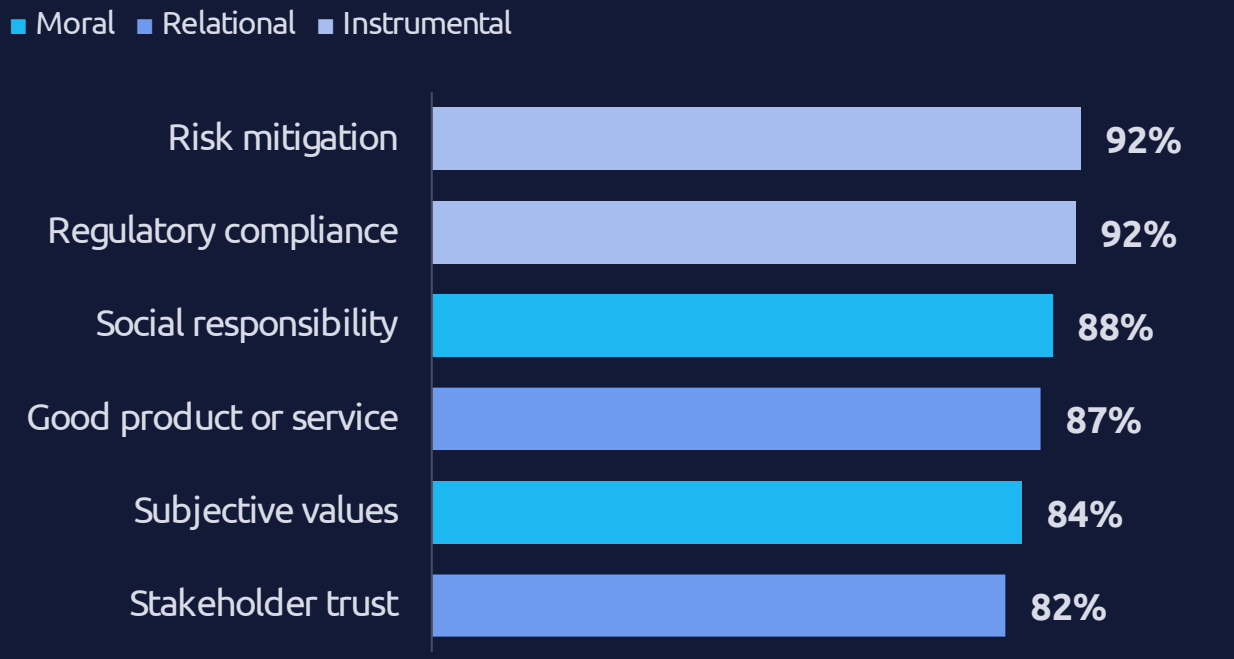
50%
strongly agree

Instrumental

79%
agree

35%
strongly agree

Six most-endorsed incentives



The results of our study challenge the view that PET adoption is driven solely by self-interest.

Source: Klymenko, A. et al.: *Investigating the Motivational Factors Influencing Managerial Decisions to Adopt Privacy-Enhancing Technologies.* In: 32nd European Conference on Information Systems (ECIS), 2024

Legal Perspective



Our work promotes PETs as effective technical measures for operationalizing Privacy by Design and supporting compliance

The legal perspective

To address the legal perspective, we built on the concept of **Privacy by Design (PbD)**, which became a **legal obligation under Article 25 of the GDPR**

- Represents a **proactive approach** to embedding privacy considerations into the design of IT systems

PbD principles leave **many open questions about their application when engineering systems**

- It is therefore often **unclear what a request for PbD practically means**

Translating PbD-based privacy requirements into PET implementations remains a **major challenge**

What exactly does PbD mean in practice and how can PETs contribute to PbD adherence?

Source: Klymenko, A. et al.: *Breaking Down Privacy by Design: A Threefold Perspective.* In: 30th Americas Conference on Information Systems (AMCIS), 2024

We showed how PETs can support adherence to Privacy by Design by mapping applicable PbD principles to the characteristics of PETs

PET and PbD mapping



Differential Privacy (DP)

Supported Principle	Supported By
(P1) Proactive not Reactive; Preventative not Remedial	Adding calibrated noise to dataset queries through DP techniques, organizations can ensure privacy and confidentiality from the very beginning in a proactive manner.
(P3) Privacy Embedded into Design	By lessening the likelihood of reidentification of individuals, organizations can ensure that privacy is protected from the moment data is collected.
(P4) Full Functionality, Positive-Sum not Zero-Sum	By controlling the amount of noise added to the data, organizations can achieve an appropriate balance that protects privacy while still enabling meaningful analysis and decision-making.
(P5) End-to-end Security - Full Life Cycle Protection	Ensuring privacy protection by adding carefully calibrated noise to the query results or aggregated information during the collection and processing of data, and protecting data against reidentification or information leakage, it contributes to full life cycle protection.
(P7) Respect for User Privacy - Keep it User-Centric	Providing an assurance that participation in a database, as well as the data itself, is less likely to be traced back to individuals.

Similar mappings have been created for the five PETs introduced earlier in the talk.

Source: Klymenko, A. et al.: *Breaking Down Privacy by Design: A Threefold Perspective.* In: 30th Americas Conference on Information Systems (AMCIS), 2024

Technical Perspective



A gap between PETs and engineering practice leaves developers uncertain how to use them

The technical perspective

To address the technical perspective, we investigated how exactly PETs can be integrated into the software engineering process

Literature supports our identified challenges, highlighting key technical barriers to PET adoption:

- A **disconnect** between PETs and **systematic engineering practice**
- **Lack of practical guidance for software developers** implementing PETs

As a result, developers are **uncertain when and how to apply PETs** in practice

How can developers be supported in applying PETs within standard software engineering workflows?

Source: Klymenko, A. et al.: *Supporting the Integration of Privacy-Enhancing Technologies into the Software Development Life Cycle.* In: SN Computer Science 6(6), 2025

Integrating PETs requires concrete activities at every stage of the development lifecycle

PET implementation activities

Planning → **Analysis** → **Design** → **Implementation** → **Testing & Integration** → **Maintenance**

- Define project scope and business goals
- Undergo initial risk assessment
- Map privacy risks to protection goals
- Derive legal requirements

- Identify technical measures: **consider PETs**
- Decide: build in-house or buy
- Design and implement the system
- Review design for compliance

- Test the system and PET impact
- Report to legal team and customers
- Optional: get a privacy compliance certification
- Check regularly for new requirements and attacks

Source: Klymenko, A. et al.: *Supporting the Integration of Privacy-Enhancing Technologies into the Software Development Life Cycle.* In: SN Computer Science 6(6), 2025

Our process diagram gives stakeholders a clear step-by-step path to integrating PETs into the software engineering process

Process diagram: PETs in Software Engineering

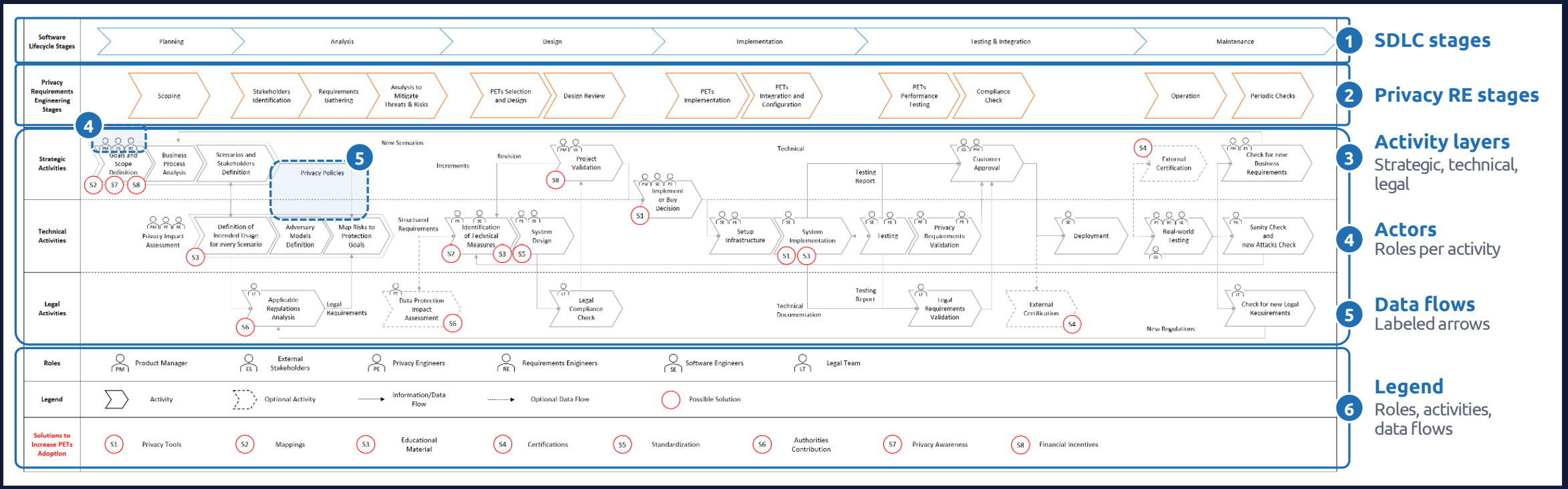
First version shaped by

1 Insights from the literature
Including previous works employing similar approaches

2 Insights from interviews
With technical practitioners

Iteratively refined

3 Revisions
After feedback from technical practitioners



Source: Klymenko, A. et al.: *Supporting the Integration of Privacy-Enhancing Technologies into the Software Development Life Cycle.* In: SN Computer Science 6(6), 2025

PET adoption needs various stakeholders working together

Ways to contribute to PET adoption

Set the rules

Governments and standards bodies

Set the floor: clear rules and enforcement, standards, certification schemes and funding

Legal professionals

Translate regulation into concrete requirements and audit compliance

Make it possible

Technical professionals

Build and apply usable PET tools and carry out the implementation in systems

Academia

Produce mappings, education and open-source tooling; turn research into practice

Drive the decision

Managers

Decide budgets, set the privacy ambition and lead by example (tech leaders)

End users

Create demand for privacy-friendly products and expect transparency on data use

Let's move PETs from promise to practice, together ☺

Feel free to explore our practitioner-focused resources developed from the findings of our research work

Resources

White paper

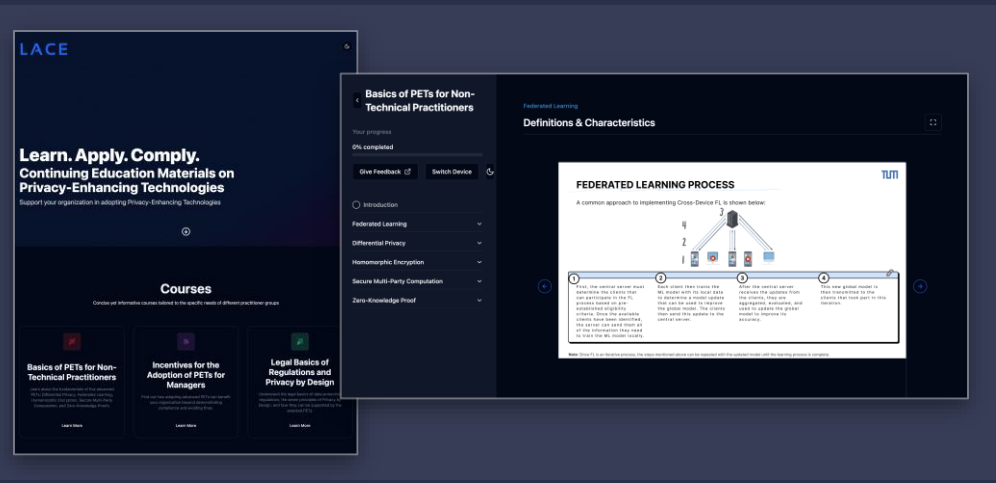
Privacy-Enhancing Technologies: A Comprehensive Guide for Non-technical Practitioners



Scan to access the white paper

Learning platform

Free courses for practitioners: PET basics, incentives for managers, legal basics



Scan to access the learning platform

https://privacyeducation.tech/

Bonus: PETs and AI



AI raises privacy stakes while the strongest PETs still remain largely unused

AI privacy risks and mitigations

Why AI raises risk

Wider access

More capable models

More data in use

Where PETs come in

Risk addressed	PET	Status	Verdict
Training-data exposure	**Synthetic Data**	**Mainstream**	Easy to adopt No formal guarantees
Memorization and leakage	**Differential Privacy**	**Limited**	Strong guarantees Utility trade-off
Centralized raw data	**Federated Learning**	**Limited**	Keeps data local Complex to deploy
Processing sensitive data	**Homomorphic Encryption**	**Unused**	Strong protection Costly and slow
Sensitive prompts and inputs	**Private Inference**	**Unused**	Promising Little practical uptake

The adoption gap

Standard practice
Data cleaning, anonymization, synthetic data

Known but rarely deployed
Differential Privacy, Federated Learning, Homomorphic Encryption, Private Inference

Barriers
Cost, utility loss, unclear regulation

Check out more details and expert insights on AI privacy risks and mitigation strategies in our paper.

Source: Klymenko, A. et al.: *"We are not Future-ready": Understanding AI Privacy Risks and Existing Mitigation Strategies from the Perspective of AI Developers in Europe.* In: 21st Symposium on Usable Privacy and Security (SOUPS), 2025

Thank you!

Open to your questions and discussion

Get in touch

Dr. Alexandra Klymenko, CIPM

alexandra.klymenko@capgemini.com / @tum.de

linkedin.com/in/alexandra-klymenko

Happy to connect on LinkedIn