TECH HIVE
ADVISORY

Article

Advancing Trustworthy AI through

Privacy-Enhancing Technologies in Africa

```
    free_page((unsigned long)group_info->blocks[i]);
  }
  kfree(group_info);

  return NULL;
}

EXPORT_SYMBOL(groups_alloc);

void groups_free(struct group_info *group_info)
{
  if (group_info->blocks[0] != group_info->small_block)
    int i;
    for (i = 0; i < group_info->nblocks; i++)
      free_page((unsigned long)group_info->blocks[i]);
```

Introduction

As Artificial Intelligence (AI) powered technologies continue to advance and transform industries, companies need access to large data sets to train and improve AI models. However, when these datasets include personal information, the stakes become higher. This raises an important question: how is the data used to build and run AI systems being protected? People want to know what safeguards exist to ensure their information is not misused or exposed.

How should companies balance the need to access and share data to develop and improve AI with the equally critical need to protect personal information? One promising solution lies in Privacy Enhancing Technologies (PETs). PETs offer practical ways to reconcile the demand for data in AI with the important need for data protection and compliance.

What are Privacy Enhancing Technologies (PETs)?

While there is no standard definition of PETs as it has been defined in various ways by organisations, the main goal of PET is to safeguard data without exposing sensitive information when the data is being shared. Thus, PETs can be defined as tools and techniques that protect data using a privacy by design approach.[1] In simple terms, PETs allow organisations to make use of valuable data whether for decision-making, analytics, or training AI models while protecting the data.[2] They make it possible to harness the the value of data for AI development without compromising compliance or individual rights.

[1] 'Privacy-Enhancing Technologies: Global and Cross-Sectoral Regulatory Insights' (Data Security Council of India (DSCI, 6 April 2024)) <https://www.dsci.in> accessed 12 September 2025

[2] 'Sharing trustworthy AI models with privacy-enhancing technologies'/ (OECD (2025), OECD Artificial Intelligence Papers, No. 38, OECD Publishing, Paris, <https://doi.org/10.1787/a266160b-en> accessed 12 September 2025.

PETs can be grouped into two broad categories: those designed for input privacy and those designed for output privacy. [3] Input privacy ensures that sensitive data remains protected during processing, whether handled by one party or across multiple parties, so the raw information cannot be misused outside its defined context. Techniques such as secure multiparty computation (SMPC) and homomorphic encryption allow computations without exposing the underlying data. Output privacy, by contrast, safeguards the results of computation by modifying them so that they cannot be used to re-identify or reverse engineer the original inputs. [4] Methods like differential privacy or synthetic data generation are commonly used for this purpose. Taken together, these approaches enable safer data life cycles, strengthen compliance with data protection laws, and foster trust in AI-driven systems.

Some examples of PETs include:

1. **Differential privacy:** This adds "noise" (mathematical adjustments) to datasets so individual information is hidden while still preserving overall patterns. For instance, Apple has been reported to use differential privacy in iOS to collect usage statistics (like emoji preferences) without tying them back to individuals. [5]

2. **Federated learning:** This involves training AI models across multiple devices or organisations without raw data ever leaving its source. Google discloses it uses federated learning in Gboard (its keyboard app), so the model learns from millions of users' typing patterns without sending individual keystrokes to Google's servers. [6]

3. **Homomorphic encryption (HE):** This allows computations to be performed directly on encrypted data without decrypting it. One example is the use of HE by IBM researchers where they applied machine learning to fully encrypted banking data using a homomorphic encryption scheme, and the predictions were stated to be as accurate as those made with unencrypted data. [7]

4. **Secure multiparty computation (SMPC):** This enables parties to work on shared data without revealing it to each other. For instance, multiple banks can collaborate by sharing sensitive financial transaction data to detect money laundering. Using SMPC, they can run analytics on the combined dataset without exposing their customers' raw data to one another. [8]

[3] 'The United Nations Guide on Privacy-Enhancing Technologies for Official Statistics' (United Nations Committee of Experts on Big Data and Data Science for Official Statistics, New York, 2023) <https://unstats.un.org/bigdata/events/2023/unsc-pet-guide/> accessed 12 September 2025

[4] ibid.

[5] 'Learning with Privacy at Scale' (Apple Machine Learning Research, 6 December 2017) <https://machinelearning.apple.com/research/learning-with-privacy-at-scale> accessed 12 September 2025

[6] 'Learn How Gboard Gets Better - Gboard Help' <https://support.google.com/gboard/answer/12373137?hl=en> accessed 13 September 2025

[7] 'The Future of Crypto: IBM Makes a New Leap with Fully Homomorphic Encryption' (IBM Research, 17 December 2020) <https://research.ibm.com/blog/fhe-progress-milestones> accessed 14 September 2025

[8] 'Confidential Computing Use Cases' (Microsoft Azure, 7 May 2025) <https://learn.microsoft.com/en-us/azure/confidential-computing/use-cases-scenarios> accessed 14 September 2025

5. **Synthetic data:** This is artificially generated data that mimics the patterns and characteristics of real data but does not contain actual personal information. Synthetic data is often used in AI and machine learning to create training datasets when real data is limited or too sensitive to use. [9] For example, instead of using real patient health records, a hospital can create synthetic data that looks and behaves like the original but doesn't expose anyone's personal information. This allows organisations to train AI models, test systems, or share datasets safely without risking privacy breaches.

6. **Trusted execution environments (TEEs):** A TEE is a secure area inside a computer's processor that ensures data is processed in a protected space, isolated from the rest of the system. TEEs are especially useful when running AI models on cloud platforms, because they allow data to be processed securely even on third-party infrastructure. [10] In Singapore's PET Sandbox initiative, a pharmaceutical distributor used TEEs to combine data from multiple partners for disease trend analysis, without sharing raw datasets. [11]

Other categories of PETs include encryption, which ensures that data is scrambled and accessible only to authorised parties; anonymisation, which eliminates identifiable information from datasets to prevent re-identification; and pseudonymisation, which substitutes identifying details with pseudonyms. [12]

Adopting PETs for Development of AI Systems

PETs are essential tools for the development of AI systems because they make it possible to access and use diverse and high quality data sets while safeguarding sensitive information. Although PETs are still evolving and have their shortcomings, combining different techniques often provides stronger protection for personal data than relying on a single method. [13] This layered approach helps to mitigate the individual limitations of each PET and ensures more robust privacy. [14] Some of the key reasons companies should adopt PETs include;

[9] 'What Are Privacy-Enhancing Technologies?'(Decentriq, 16 April 2025) <https://www.decentriq.com/article/what-are-privacy-enhancing-technologies> accessed 14 September 2025w York, 2023) <https://unstats.un.org/bigdata/events/2023/unsc-pet-guide/> accessed 12 September 2025

[10] 'Sharing trustworthy AI models with privacy-enhancing technologies'/ (OECD (2025), OECD Artificial Intelligence Papers, No. 38, OECD Publishing, Paris, <https://doi.org/10.1787/a266160b-en> accessed 15 September 2025.

[11] 'Accessing More Data Through Trusted Execution Environment to Generate New Insights' (Infocomm Media Development Authority) <https://www.imda.gov.sg/-/media/imda/files/programme/pet-sandbox/jan2024_imda-pet-sandbox-case-study-healthcare-services.pdf> accessed 15 September 2025.

[12] 'LibGuides: Data Management for Students: Anonymisation, Pseudonimisation & Encryption' (Tilburg University) <https://libguides.uvt.nl/rdmstudent/anonymisation> accessed 16 September 2025

[13] 'n 10.

[14] 'Liv d'Aliberti, Evan Gronberg and Joseph Kovba, 'Privacy-Enhancing Technologies for Artificial Intelligence-Enabled Systems' (arXiv, 4 April 2024) <http://arxiv.org/abs/2404.03509> accessed 16 September 2025.

Foster trust

PETs foster trust by assuring individuals that their personal data is protected. [15] When people know that their information will not be misused or exposed, they are more willing to share data. This trust directly contributes to the development and deployment of quality AI systems trained on richer datasets.

Promote collaboration

Beyond protecting the information of individuals, PETs also promote collaboration among researchers, companies, and institutions. PETs reduce the risks of exposing proprietary information or violating data protection rules by enabling safe sharing and joint use of sensitive data. [16] Technologies like synthetic data or differential privacy allow AI models to be trained without revealing the underlying raw data. Similarly, federated learning supports collaborative analysis across multiple entities without requiring centralised data pooling. [17] This makes cross-border and cross-sector partnerships more feasible and secure.

Safeguard personal d ata

Data protection laws mandate organisations to safeguard personal data. PETs can play a critical role in meeting these legal obligations by embedding data protection-by-design principles into AI systems. [18] Furthermore, data breaches and misuse carry significant financial and reputational costs. PETs minimise the risk of exposure by ensuring that sensitive data is never fully revealed, even during analysis or model training. [19] This makes PETs a cost-effective approach to risk management.

Drive innovation

Finally, PETs allow sensitive data such as health records, financial transactions, or educational data to be used in AI systems without compromising privacy. This can drive innovation across sectors such as healthcare, fintech, and education while ensuring safety and compliance by enabling access to diverse and high-quality datasets. [20]

....

[15] ‘Privacy Enhancing Technologies’ (Future of Privacy Forum) <https://fpf.org/issue/privacy-enhancing-technologies/> accessed 28 September 2025

[16] 'Sharing trustworthy AI models with privacy-enhancing technologies'/ (OECD, 17 June 2025), OECD Artificial Intelligence Papers, No. 38, OECD Publishing, Paris, <https://doi.org/10.1787/a266160b-en> accessed 15 September 2025.

[17] 'ibid.

[18] Exploring Practical Considerations and Applications for Privacy Enhancing Technologies’ (31 May 2024,ISACA) <https://www.isaca.org/resources/white-papers/2024/exploring-practical-considerations-and-applications-for-privacy-enhancing-technologies> accessed 16 September 2025.

[19] 'Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age' (Centre for Information Policy Leadership, December 2023) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf> accessed 16 September 2025.

[20] ibid.

Choosing the Right PET(s) For AI Systems

PETs vary in the level of protection they provide and the functions they perform. It is therefore essential for organisations to carefully identify and adopt PETs that align with their operational and compliance requirements. The following considerations are important when making this choice:

Understand the AI system's use case

Understanding the purpose of the AI system is the starting point for choosing the right PET. By clearly defining the objectives, risks, and compliance needs, companies can select PET(s) that protects data while supporting efficiency, trust, and regulatory obligations. Without this clarity, organisations risk adopting tools that either over-engineer protection at the cost of efficiency or, worse, under-protect against significant vulnerabilities. [21] It is also important to note that not all data requires the same level of protection. Highly sensitive categories such as health, or biometric information demand advanced PETs that provide mathematically provable guarantees, like SMPC or homomorphic encryption. [22] By contrast, less sensitive data such as aggregated weather patterns may be adequately safeguarded through anonymisation or pseudonymisation. This illustrates why a clear understanding of the AI system is essential for selecting the right PET.

Conduct a data protection impact assessment (DPIA)

A formal DPIA is critical for identifying data protection risks, mapping how personal data is processed, and evaluating whether PETs can mitigate those risks.[23] The assessment should address practical questions: What needs to be protected, and from whom? Are multiple parties contributing data, and can they trust each other? The answers shape whether input privacy methods like secure multiparty computation (sMPC) or homomorphic encryption are appropriate, or whether output-focused approaches like differential privacy would suffice. [24]

[21] Liv d'Aliberti, Evan Gronberg and Joseph Kovba, 'Privacy-Enhancing Technologies for Artificial Intelligence-Enabled Systems' (arXiv, 4 April 2024) <http://arxiv.org/abs/2404.03509> accessed 16 September 2025.

[22] Exploring Practical Considerations and Applications for Privacy Enhancing Technologies' (31 May 2024,ISACA) <https://www.isaca.org/resources/white-papers/2024/exploring-practical-considerations-and-applications-for-privacy-enhancing-technologies> accessed 17 September 2025.

[23] 'ibid.

[24] 'The United Nations Guide on Privacy-Enhancing Technologies for Official Statistics' (United Nations Committee of Experts on Big Data and Data Science for Official Statistics, New York, 2023) <https://unstats.un.org/bigdata/events/2023/unsc-pet-guide/> accessed 12 September 2025

The recently published Ghana Draft Data Protection Bill 2025 provides that a DPIA must be conducted before the deployment of emerging technologies. [25] Also, article 43(4) of the Nigerian Data Protection Act General Application and Implementation Directive 2025 (GAID) requires companies deploying emerging technologies such as AI to carry out a DPIA before deployment for high risk systems. [26] The DPIA must go beyond surface-level risk mapping to specifically assess whether the processing could lead to unfair or unequal outcomes for different groups, and consider how vulnerable certain categories of data subjects may be by using tools like the Data Subjects' Vulnerability Index (DSVI). [27]

Under the Botswana Data Protection Act 2024, data controllers are required to conduct a DPIA before engaging in any data processing activity involving new technologies that is likely to pose a high risk to individuals' rights and freedoms.[28] This includes large scale automated decision making or profiling of natural persons and systematic monitoring of public spaces on a large scale. [29]

Furthermore, section 30 of the Malawi Data Protection Act 2024, article 47 of the Ethiopia Personal Data Protection Proclamation 2024, and section 40 of the Republic of Seychelles Data Protection Act 2023 require data controllers to conduct a DPIA before undertaking any processing activity likely to present a high risk to the rights and freedoms of individuals, such as automated decision-making, profiling, or large-scale monitoring of public spaces.

Evaluate operational, technical, and resource constraints

The environment in which PETs operate matters. Some PETs such as differential privacy are flexible and can be integrated across a wide range of systems. Others, like TEEs, require specific hardware or cloud infrastructure to function effectively. Businesses must also consider scalability and whether PETs can integrate smoothly with authentication, identity management, and key management systems already in place. [30]

It is also important to consider the relevant resources and expertise available as advanced cryptographic PETs such as homomorphic encryption or sMPC often require specialised skills and can be cost-intensive, while more solutions like differential privacy may be supported by off-the-shelf tools and service providers. [31]

[25] Ghana Data Protection Draft Bill, sec 53(7)

[26] General Application and Implementation Directive 2025, art 44(4)(a)

[27] General Application and Implementation Directive 2025, art 44(4)(a)(i).

[28] Botswana Data Protection Act 2024, sec 65(1)

[29] Botswana Data Protection Act 2024, sec 65(2)

[30] 'Exploring Practical Considerations and Applications for Privacy Enhancing Technologies' (31 May 2024,ISACA) <https://www.isaca.org/resources/white-papers/2024/exploring-practical-considerations-and-applications-for-privacy-enhancing-technologies> accessed 17 September 2025.

[31] The United Nations Guide on Privacy-Enhancing Technologies for Official Statistics' (United Nations Committee of Experts on Big Data and Data Science for Official Statistics, New York, 2023) <https://unstats.un.org/bigdata/events/2023/unsc-pet-guide/> accessed 18 September 2025.

Consider interoperability and hybrid approaches

Some PETs complement each other and can be combined to achieve stronger or more flexible protection. For example, synthetic data can be enhanced with differential privacy, while sMPC can be paired with homomorphic encryption. [32] For many businesses, exploring hybrid models provides a practical balance between security, efficiency, and usability.

Finally, organisations must recognise that PETs are not static solutions. Technology evolves, regulations shift, and new risks emerge. A forward-looking PET strategy should include provisions for continuous monitoring, independent oversight, and adaptability to changing regulatory landscapes. The Nigerian GAID reinforces this by requiring data controllers to establish mechanisms for ongoing monitoring and evaluation of emerging technologies even after deployment. [33]

Regulatory Drivers

Data protection laws across several African countries are increasingly emphasising the adoption of PETs such as encryption, anonymisation, and pseudonymisation to ensure the secure and responsible processing of personal data. In Ghana, the draft Data Protection Bill 2025 explicitly requires the use of PETs to ensure transparency and accountability in automated decision-making processes. [34]

Data protection laws across several African countries are increasingly emphasising the adoption of PETs such as encryption, anonymisation, and pseudonymisation to ensure the secure and responsible processing of personal data.[35] In Ghana, the draft Data Protection Bill 2025 explicitly requires the use of PETs to ensure transparency and accountability in automated decision-making processes. Similarly, the Kenya Data Protection Act 2019 mandates data controllers and processors to implement appropriate technical and organisational measures for the protection of personal data. [36]

[32] 'Sharing trustworthy AI models with privacy-enhancing technologies'/ (OECD (2025), OECD Artificial Intelligence Papers, No. 38, OECD Publishing, Paris, <https://doi.org/10.1787/a266160b-en> accessed 15 September 2025.

[33] General Application and Implementation Directive 2025, art 43(4)(e)

[34] Ghana Draft Data Protection Bill 2025,section 53(3)

[35] Kenyan Data Protection Act 2019, s 41

[36] Kenyan Data Protection (General) Regulations 2021, reg 27

In Malawi, the Data Protection Act 2024 states that the data protection authority should promote the development and adoption of personal data protection technologies that align with international standards and relevant international laws. [37] Mauritius also published a Guide on Data Protection for Health Data and Artificial Intelligence Solutions in 2020 which emphasised the use of data anonymisation and pseudonymisation techniques to ensure the responsible use of AI. [38]

The Egypt National AI Strategy calls for the implementation of stringent data security measures, including encryption and data anonymisation to protect personal and sensitive data when enabling data accessibility and sharing in the development and deployment of AI technologies. [39] In Tanzania, the Draft Guidelines for the Secure and Ethical Use of AI recommend that organisations should develop data stores that support data encryption, anonymisation and pseudonymisation, and integration with the data catalogue. [40]

Furthermore, the draft revision of the Personal Data Protection Law, Angola also introduces comprehensive safeguards for the processing of personal data by AI systems, including encryption and pseudonymisation which should commensurate with the level of risk associated with the processing activities. [41]

The General Application and Implementation Directive 2025 (GAID) under the Nigeria Data Protection Act (NDPA) provides a clear legal foundation for the safe deployment of data-driven systems, including AI. Article 31 of the GAID requires data controllers and processors deploying software that processes personal data such as operating systems, mobile applications, or AI systems to embed privacy by design and by default through appropriate technical and organisational measures. [42] Deployers of emerging technologies, including AI, are further required to evaluate the suitability of anonymisation when collecting data and to test such technologies in controlled, low-risk environments. [43]

It is also important to note that Article 43 of the GAID recognises synthetic data and tokenisation as privacy-enhancing alternatives to raw personal data. These techniques allow organisations to reduce direct reliance on identifiable information while still enabling AI development and deployment. However, the regulation also acknowledges an important limitation synthetic data and tokenised data may not always be amenable to the right to be forgotten. [44] Thus, while PETs reduce privacy risks, they do not eliminate them and data controllers must still ensure that synthetic or tokenised datasets do not undermine data subject rights.

[37] Malawi Data Protection Act 2024, s 5(2)(c)

[38] 'Guide on on Data Protection for Health Data and Artificial Intelligence Solutions' (Data Protection Office, Mauritius, 17 April 2020) <https://dataprotection.govmu.org/Communique/Guide%20on%20Data%20Protection%20for%20health%20data%20and%20AI.pdf> accessed 20 October 2025

[39] 'Egypt National Artificial Intelligence Strategy, Second Edition (2025 - 2030)'<https://ai.gov.eg/SynchedFiles/en/Resources/AIstrategy%20English%2016-1-2025-1.pdf>accessed 20 October 2025.

[40] 'Guidelinefor the Secure and Ethical Use of Artificial Intelligence in Tanzania' (Ministry of Information, Communication & Information Technology, June 2024) <https://www.mawasiliano.go.tz/uploads/documents/sw-1749982790-Guidelines%20for%20AI%20ethical%20USE%20Guideline%20MICIT%202025ver.pdf> accessed October 20 2025.

[41] Draft revision of the Personal Data Protection Law, Angola, art 39 and 40

[42] General Application and Implementation Directive 2025, art 31(2)(e)(v).

[43] General Application and Implementation Directive 2025, art 43(4)(b)

[44] General Application and Implementation Directive 2025, art 43(2)(b)

Finally, Article 44 of the GAID makes it clear that the Nigeria Data Protection Commission shall foster the development of personal data protection technologies to ensure sensitive data is processed in ways that respect individual rights while still enabling innovation.

Building on these provisions, PETs such as anonymisation, pseudonymisation, and tokenisation can support compliance by reducing data identifiability while maintaining its utility for AI development. However, whether anonymised data falls outside data protection rules ultimately depends on the applied legal test, specifically, whether individuals can still be reasonably identified despite these safeguards.[45] Studies have repeatedly shown that datasets considered "anonymous" can often be re-identified when combined with other publicly available information. For instance, researchers were able to deanonymise a supposedly anonymised health billing dataset and even a Netflix film rating dataset by comparing the ratings with public scores on IMDb film website. This demonstrates that anonymisation is not an absolute guarantee of privacy. [46]

Challenges of Implementing PETs in AI Systems

While the benefits of PETs have been outlined, their adoption is not without difficulties. Implementing PETs in AI systems presents several challenges. One challenge is the lack of regulatory framework and standards. The regulatory framework for PETs is still in its early stages. There are no specific rules that directly govern their use, so companies often have to rely on broader data protection laws that make only passing reference to PETs. Some data protection authorities have gone a step further by issuing guidelines and notes to encourage their adoption. In addition, the lack of a common framework or set of technical standards makes consistent implementation difficult. [47]

Another key challenge is the high cost of PETs. Their technical demands and associated expenses can be prohibitive, particularly for smaller organisations. Obfuscation measures such as anonymisation often involve complex processes that require trained data scientists to ensure that no information is unintentionally leaked. [48]

[45]'Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age'(Centre for Information Policy Leadership, December 2023) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf> accessed 19 September 2025.

[46]Alex Hern, '"Anonymised" Data Can Never Be Totally Anonymous, Says Study' (The Guardian, 23 July 2019) <https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds> accessed 29 October 2025

[47] 'Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age'(Centre for Information Policy Leadership, December 2023) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf> accessed 19 September 2025.

[48]'Exploring Practical Considerations and Applications for Privacy Enhancing Technologies' (31 May 2024,ISACA) <https://www.isaca.org/resources/white-papers/2024/exploring-practical-considerations-and-applications-for-privacy-enhancing-technologies> accessed 16 September 2025.

Another challenge lies in the fact that a single PET is rarely sufficient to address all data protection concerns in an AI system. PETs are often use-case specific, with some proving more effective in particular scenarios than others and each comes with its own limitations and risks.[49] For example, synthetic data and differential privacy can reduce re-identification risks but may introduce bias or degrade model accuracy. Homomorphic encryption enables secure computation but is computationally expensive, while multi-party computation reduces data leakage risks in federated learning but often suffers from high communication overhead. [50] Because PETs are frequently complementary, organisations may need to combine multiple PETs to achieve the desired outcome.

In addition to the above-mentioned challenges, PETs do not necessarily resolve deeper issues such as biases embedded in the original data, nor can they guarantee the security of the broader IT systems that rely on the protected data.[51] Even commonly used techniques like anonymisation are not fully reliable, as records can often be re-identified after release. [52] This is largely because it is impossible to anticipate every dataset that might later be combined with anonymised data or the future technologies and analytical methods that could enable re-identification.

A growing concern in the adoption of PETs is the risk of "PET-washing". This occurs when organisations misrepresent or exaggerate their use of PETs to appear privacy-conscious or compliant, while their underlying practices remain ineffective or unethical. An organisation may claim to use anonymisation or federated learning to protect personal data, even though such implementations may still allow data re-identification or fail to meet legal and ethical standards. This could also be attributed to the absence of universal standards and verification mechanisms for PET deployment which makes it difficult to distinguish genuine PETs from superficial compliance claims.

Further compounding the issue, the highly technical and fast evolving nature of PETs not only makes implementation difficult for many organisations but also complicates their integration into policy and legal frameworks governing data use. [53]

Together, these challenges highlight that PETs while valuable, cannot be considered a complete solution to the data protection risks inherent in AI systems and must be implemented strategically to ensure effective and responsible deployment.

[49] 'Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age' (Centre for Information Policy Leadership, December 2023) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf> accessed 19 September 2025.

[50] 'Sharing trustworthy AI models with privacy-enhancing technologies'/ (OECD, 17 June 2025), OECD Artificial Intelligence Papers, No. 38, OECD Publishing, Paris, <https://doi.org/10.1787/a266160b-en> accessed 20 September 2025.

[51] 'Emerging privacy-enhancing technologies: Current regulatory and policy approaches' (OECD, 8 March 2023),OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, <https://doi.org/10.1787/bf121be4-en> accessed 20 Septermber 2025.

[52] Luc Rocher Julien M Hendrickx and Yves-Alexandre de Montjoye, 'Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models' (2019) 10 Nat Commun 3069 <https://www.nature.com/articles/s41467-019-10933-3> accessed 21 September 2025.

[53] 'Emerging privacy-enhancing technologies: Current regulatory and policy approaches' (OECD, 8 March 2023),OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, <https://doi.org/10.1787/bf121be4-en> accessed 20 Septermber 2025.

Recommendations for the Effective Implementation of PETs in AI Systems

Despite the challenges involved in the implementation of PETs mentioned above, PETs are essential for building safer and more trustworthy AI systems, particularly in contexts where sensitive data is involved. To address these issues, the following recommendations are hereby proposed to guide organisations, policymakers, and regulators in the effective adoption and deployment of PETs.

One of the most pressing needs is for clearer and more practical regulatory guidance. Regulators should take a risk-based approach in evaluating PETs, especially when it comes to standards for anonymisation and compliance with data protection rules. [54] Regulators can reduce uncertainty and enable organisations to adopt PETs more confidently by avoiding rigid, one-size-fits-all requirements. [55]

Promoting adoption also requires supportive policy mechanisms. Governments can play a role through experimental regulation, such as regulatory sandboxes and innovation contests, all of which allow safe experimentation while lowering barriers to scale. [56] These efforts need to be coupled with the development of shared technical standards and interoperability frameworks. The lack of consistent benchmarks across PETs remains a major barrier, and establishing common guidelines would enable tools to work seamlessly across jurisdictions while providing clearer metrics for transparency, accountability, and performance. [57]

To mitigate the growing risk of "PET-washing", regulators and standard-setting bodies should introduce verification and certification mechanisms for PETs. These mechanisms would enable independent evaluation of PET implementations to confirm that they meet recognised technical, ethical, and legal standards. Such frameworks could include data protection impact assessments, third-party audits, or trust marks that validate genuine implementations and prevent superficial or misleading claims of data protection in AI systems. Establishing clear benchmarks and transparent reporting requirements would further discourage superficial compliance and promote genuine, accountable adoption of PETs in AI development and deployment. Organisations, policymakers, and service providers should collaborate to develop scalable and cost-effective infrastructure for PET development and deployment.

[54] 'Sharing trustworthy AI models with privacy-enhancing technologies'/ (OECD, 17 June 2025), OECD Artificial Intelligence Papers, No. 38, OECD Publishing, Paris, <https://doi.org/10.1787/a266160b-en> accessed 21 September 2025.

[55] ibid.

[56] 'Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age' (Centre for Information Policy Leadership, December 2023) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf> accessed 20 September 2025.

[57] ibid.

This could include open-source initiatives, subsidised access to high-performance computing resources, shared cloud platforms, or public-private partnerships that lower barriers for smaller enterprises. Additionally, investing in optimisation techniques and efficient implementations of resource-intensive PETs can help reduce computational overhead without compromising data protection. [58]

Capacity building is equally important. Many organisations lack the awareness or expertise needed to implement PETs effectively. Expanding training programmes, certification schemes, and awareness campaigns can help bridge this gap and ensure that technical skills keep pace with technological advances. [59]

Finally, transparency and continuous improvement are vital for long-term trust. PETs can be complex and difficult to explain, but organisations should nevertheless strive to provide clear and contextually appropriate communication about their use, benefits, and limitations. This helps build confidence among users, regulators, and the public. [60] At the same time, PETs are not static technologies; they evolve rapidly, and ongoing investment in research, pilot projects, and benchmarking initiatives is necessary to keep them effective against emerging risks. Stakeholders can ensure that PETs contribute meaningfully to safer and more responsible AI systems by committing to continuous improvement and open communication.

Conclusion

PETs are critical tools for deploying safer and more trustworthy AI systems. PETs offer significant potential to advance privacy by design principles, promote trust in sharing data and enable innovative AI-driven solutions across various sectors. However, their effective adoption requires careful consideration of technical limitations, computational requirements, use-case specificity, and regulatory guidance. To realise their full potential, organisations must integrate PETs into a broader privacy and data governance framework, supported by collaboration among technical teams, policymakers, and management. In doing so, PETs can serve as a foundational component in building AI systems that are innovate, safe and responsible, helping to balance the competing demands of data protection and innovation.

Author: **Rodiyyah Bashir** | Editor: **Ridwan Oloyede**

[58] 'Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age' (Centre for Information Policy Leadership, December 2023) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf> accessed 20 September 2025.

[59] 'Sharing trustworthy AI models with privacy-enhancing technologies'/ (OECD, 17 June 2025), OECD Artificial Intelligence Papers, No. 38, OECD Publishing, Paris, <https://doi.org/10.1787/a266160b-en> accessed 21 September 2025.

[60] ibid.