Data Privacy & Protection
8th April 2024

Sandra Eke

THE ROLE OF PRIVACY ENHANCING TECHNOLOGIES (PETs) IN ATTAINING DATA PROTECTION COMPLIANCE IN NIGERIA[1]

1. Introduction

Personal data security is paramount in safeguarding individuals' privacy, fostering trust in digital interactions, ensuring legal compliance, preserving business continuity, and protecting against cyber threats.[2] By prioritizing data security measures and adopting a proactive approach to risk management, organizations can uphold their obligations to data subjects, maintain their reputation, and thrive in today's digital world through the use of privacy-enhancing technologies (PETs). PETs adopt engineered systems such as secure multiparty computations, homomorphic encryption, anonymisation, differential privacy, mix networks, anonymous digital credentials etc., that provide acceptable levels of privacy.[3] They are information security techniques that enhance privacy, protects and reduces the risk of personal data exposure to unauthorized third parties.[4] They incorporate primary data protection principles by minimising the usage of personal information, maximising data security, and empowering data subjects.[5] PETs play a vital role in aiding organizations achieve and maintain compliance with data protection laws and regulations, especially as it

---

1 **Sandra Eke, Associate, Intellectual Property and Technology Department, S.P.A. Ajibade & Co, Lagos, Nigeria**.

2 AI Multiple Research, "Top 10 Privacy Enhancing Technologies & Use Cases in 2024" available at: https://research.aimultiple.com/privacy-enhancing-technologies/ accessed 31st March 2024.

3 IAPP, "Privacy Program Management" 3rd Edition, Ch. 5, p. 163.

4 IBM, "Privacy Enhancing Technologies for Regulatory Compliance" available at: https://research.ibm.com/projects/privacy-enhancing-technologies-for-regulatory-compliance accessed 2nd April 2024.

5 ICO, "Guidance on Privacy-enhancing technologies (PETs) 2023" available at: https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf accessed 1st April 2024.

relates to data security. In Nigeria, the Nigeria Data Protection Act (NDPA)[6] requires data controllers/processors to implement appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of personal data in their possession or under their control, in addition to adhering to global principles of data processing.[7] PETs could help data controllers/processors under the Nigerian regulatory purview achieve compliance in this regard. In this article, we examine the benefits of PETs and how data controllers/processors can effectively leverage on these tools to attain data protection compliance in Nigeria.

2. Understanding PETs and their benefits

Privacy-enhancing technologies (PETs) are technologies, tools, techniques, and practices which are designed to protect the privacy of data subjects.[8] They achieve this by safeguarding personal data during storage, processing, and transmission. PETs include methods like encryption, anonymization, access controls, and solutions such as differential privacy, synthetic data generation, federated learning, and confidential computing as some examples.[9] They are technologies that encapsulate fundamental data protection principles by minimising personal data use, maximising data security, and empowering data subjects.[10] Knowledge of the most appropriate PET or combination of PETs to utilize for a data driven project depends on an organisation's particular circumstances. If an organisation has conducted a data protection impact assessment (DPIA), and identified risks to data subjects, then it should consider at this point whether PETs can mitigate those risks.[11]

Implementation of PETs should be considered at the design phase of a project, particularly for data-intensive projects that involve potentially risky uses of personal information.[12]

3. How Data Controllers/Processors can use PETs to enhance Compliance

---

6 Nigeria Data Protection Act (NDPA) 2023, Gazette No.119, Vol. 110 (1st July 2023).

7 See, S.24(1) & (2) NDPA and S.39(1) NDPA.

8 Decentriq, "Privacy Enhancing Technologies" available at: https://www.decentriq.com/article/what-are-privacy-enhancing-technologies#:~:text=PETs%20include%20methods%20like%20encryption,an%20increasingly%20data%2Dcentric%20world, accessed 2nd April 2024.

9 Ibid.

10 ICO, "Guidance on Privacy-enhancing technologies (PETs) 2023" available at: https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf, accessed 1st April 2024.

11 Ibid.

12 ICO, "Guidance on Privacy-enhancing technologies (PETs) 2023" available at: https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf, accessed 1st April 2024.

The Nigeria Data Protection Act requires data controllers/processors to implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data.[13] It also requires data controllers/processors to adhere to the principles of personal data processing when processing personal data.[14] PETs can assist organisations implement data protection principles effectively and integrate necessary safeguards into their processing in compliance with the statutory requirements. They can help with demonstrating a 'data protection by design and by default' approach during the processing operations of an organisation.[15] They can also help organisations comply with data minimisation principle by ensuring that personal data they process is restricted to their needed purposes, and provide an appropriate level of security for their processing.[16] By adopting PET solutions such as data anonymization and aggregation, organizations can limit the risk of data breaches and protect privacy rights of data subjects.[17]

PETs can also help controllers/processors improve the accuracy of their data and ensure that the data they collect is of high-quality and reliable.[18] They could help with data validation and ensure that data collected is accurate and complete. For instance, one privacy-enhancing technology that can be used for data validation is homomorphic encryption,[19] which can be used to validate personal data without exposing it to third parties or risking a data breach.[20]

It is important to note that PETs include privacy-focused web browsers, search engines, and communication platforms that prioritize user privacy and security. These platforms often incorporate features such as ad-blocking, tracker prevention, and decentralized architectures to minimize data collection and enhance user anonymity.[21]

4. Some types of data processing activities that could benefit from using PETs

---

13 See, S.24(1) & (2) NDPA and S.39(1) NDPA.

14 Ibid.

15 ICO, "Guidance on Privacy-enhancing technologies (PETs) 2023" available at: https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf accessed 1st April 2024.

16 Ibid.

17 Ibid.

18 ClearCode, "The Benefits of Privacy-Enhancing Technologies (PETs) In AdTech" available at:https://clearcode.cc/blog/benefits-privacy-enhancing-technologies-adtech/ accessed 2nd April 2024.

19 Homomorphic encryption enables computations on encrypted data without decrypting it first. This ensures data privacy while still allowing meaningful operations to be carried out on the encrypted information.

20 Ibid.

21 Ibid.

PETs are suitable information security measures for some types of personal data processing activities undertaken by data controllers/processors which are likely to result in a risk to the rights and freedoms of data subjects. They can help assess and mitigate risks to achieve compliance with data protection laws. The Guidance Notice released by the Information Commission Office on PETs embodies relevant examples of some data processing activities that are likely to pose risk to data subjects and how PETs can aid an organisation mitigate such risks:[22]

S/N	Processing activity	Possible risks to individuals	PETs which could aid compliance and help assess and mitigate risks
1.	Data processing involving artificial intelligence, machine learning, and deep learning applications.	Possible risks to people involved in the training dataset include model inversion, model inference and attribute inference attacks. These can reveal people's identities or may result in learning sensitive information about them.	a. Homomorphic Encryption (HE) PET ensures that only parties with the decryption key can access the information. This protects the information that is being processed (e.g., to train the AI model); b. Secure multi-party computation (SMPC) PET can protect information sent to global model; c. Differential Privacy (DP) PET adds random noise during training to ensure the final model does not memorise information unique to a particular person's personal information; d. Federated Learning (FL) PET can minimise the amount of centrally held personal information and reduce the transfer of personal information between parties; and e. Synthetic Data Generation can be used at the training stage to reduce the amount of personal information used to train artificial intelligence.
2.	Processing involving	Possible risks to people	Private-Set Intersection (PSI)

[22] ICO, "Guidance on Privacy-enhancing technologies (PETs) 2023" available at: https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf accessed 1st April 2024.

	data matching that means combining, comparing, or matching personal information obtained from multiple sources. For example, sharing financial transactions to prevent fraud and money laundering.	include collecting more information than is required for the intended purposes and security threats during transfer of personal information.	and SMPC PET can minimise the information shared and protect it during computation.
3.	Processing involving data sharing between organisations, particularly data sharing likely to result in a high risk to people.	Possible risks to people include sharing more information than the party you are sharing it with needs for their purposes, and security threats (e.g. data breaches).	SMPC, PSI and FL (when used with other PETs) can minimise the information transferred between parties. HE PET can enhance security by preventing parties accessing the input information without affecting utility.
4.	Processing involving cloud computing applications.	Possible risks to individuals include increased risk of security threats from attackers due to performing computations in untrusted environments.	Trusted execution environments (TEEs), HE and SMPC can be used for cloud computing processing tasks to provide enhanced security.
5.	Processing involving anonymisation of personal information.	Re-identification of people in information that has not been effectively anonymised.	Differential Privacy PET can prevent people from being identified in published information or limit the amount of personal information released from queries.

5. Conclusion

Privacy Enhancing Technologies represent an essential frontier in the ongoing battle to protect the personal data of individuals in the digital age. They present a vital opportunity for organizations in Nigeria to achieve data protection compliance in accordance with the Nigerian data protection legislations. By leveraging PETs, organizations can implement robust safeguards to protect personal data, mitigate privacy risks, and uphold the rights of individuals. Through mechanisms such as anonymization, encryption, access controls, and privacy by design principles, PETs enable organizations to align their data processing practices with the requirements of the NDPA. Furthermore, PETs empower organizations to foster a culture of privacy and trust, enhancing their ability to navigate the evolving regulatory landscape and build confidence among stakeholders. However, despite their promise, PETs have several challenges and limitations including complexity, compatibility with existing systems, and cost considerations, and should be used with caution. As Nigeria's data protection framework continues to evolve, the strategic adoption of PETs will

be essential for organizations seeking to demonstrate their commitment to responsible data stewardship and compliance with data protection laws.

For further information on this article and area of law
Please contact **Sandra Eke** at: S. P. A. Ajibade & Co., Lagos by
Telephone: (+234.1.270.3009; +234.1.460.5091)
Fax (+234 1 4605092)
Mobile: (+234 703 3857 874, 234 811 249 1286)
Email: seke@spaajibade.com
www.spaajibade.com