SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal
of Cryptocurrency Research
Publisher's Home Page: https://www.svedbergopen.com/

Research Paper
Open Access

Blockchain and Data Protection by Design: An Examination of The NDPA's Provisions and Best Practices

Elesho Oluwabukolami Morenike[1], Grace Ihinosen Akhihiero[2*], Okhiai Elizabeth Blessing[3], Mobolaji Oyelola Bankole[4], Adesuyi Omobolanle Blessing[5] and Adebayo Adetayo Elizabeth[6]

[1]Research Scholar, Faculty of Law, University of Ibadan, Nigeria.
[2]Research Scholar, Faculty of Law, University of Benin, Nigeria. E-mail: graceakhihiero@gmail.com
[3]Research Scholar, Afe Babalola & Co., Ibadan 200284, Oyo, Nigeria.
[4]Researcher Scholar, Faculty of Law, Igbinedion University, Okada, Nigeria.
[5]Researcher Scholar, Faculty of Law, University of Lagos, Nigeria.
[6]Researcher Scholar, Faculty of Law, Ekiti State University, Nigeria.

Article Info

Volume 4, Issue 2, December 2024
Received : 19 June 2024
Accepted : 31 October 2024
Published : 09 December 2024
doi: 10.51483/IJCCR.4.2.2024.126-134

Abstract

The Nigeria Data Protection Act (NDPA) sets a crucial precedent for data protection in Nigeria, and its provisions have far-reaching implications for blockchain technology. As blockchain technology continues to gain traction, it is essential to examine how its decentralized and transparent nature intersects with data protection and privacy. This article delves into the NDPA's provisions and best practices for implementing data protection by design in blockchain technology, ensuring the privacy and security of personal data. Our analysis highlights the importance of integrating data protection measures from the outset of blockchain project development to ensure compliance with the NDPA and protect the privacy and security of personal data. We also analyze case studies and examples of successful implementation of data protection by design in blockchain technology, highlighting the benefits and challenges of this approach. Finally, we discuss the importance of aligning blockchain technology with the NDPA's provisions and best practices, and provide recommendations for blockchain developers, organizations, and policymakers to ensure the responsible development and use of blockchain technology in Nigeria.

Keywords: *Blockchain, Data protection by design, NDPA, Privacy, Security, Data protection impact assessment, Data subject rights, Cross-border data transfers, Privacy by design, Transparency, Accountability*

1. Introduction

One of the emerging technologies disrupting the global space is the "Blockchain." Since it successful advent in 2008 when Satoshi Nakamoto created Bitcoin, blockchain technology has gathered wider views and changed

* *Corresponding author: Grace Ihinosen Akhihiero, University of Benin, Nigeria. E-mail: graceakhihiero@gmail.com*

giant industries ranging from finance to health and government. Blockchain technology is a decentralized ledger that secures data transparently using cryptography. A blockchain stores data in blocks that are linked together in a chain. It is trite to say that blockchain as a technology cannot be limited to any jurisdiction and as such can be used by any one worldwide. Nigeria is not left out in this moving disrupting train. It has moved to establish the *National Blockchain Policy* in May, 2023. Various organizations geared towards having a solid foundation of blockchain in Nigeria have also been established and they include institutions like; Stakeholders In Blockchain Technology Association of Nigeria (SIBAN), Blockchain Nigeria User Group (BNUG), Nigeria Information Technology Development Agency (NITDA).[1]

The Federal government of Nigeria promotes the adoption of this technology as it would rapidly improve the quality of services delivered by the public and private sectors, catalyze innovation, create jobs, and enhance governance which would grow the economy. It has been predicted that the blockchain technology could boost the global economy with $1.76 trillion by 2030[2] and Nigeria wants to be a future beneficiary of the golden geese. In relation to this new emerging technology, one of the key component observed to enable a smooth flow in the economy is the implementation of data protection by design. Data has become the new global oil in our digital economy and as such there must be necessary steps taken to ensure that our personal data used in the blockchain either on-chain or off-chain is protected and secured. The statement, "privacy by design" is important because, the blockchain is a distributed ledger that is permanently stored and as such if data used cannot be erased, it is necessary, we implement data privacy rules at the beginning to avoid breach and grievous legal consequences.

"Data is the digital representation of a person. It is an intellectual property of every person that requires national protection by the instant government of each state. In industry circles, consumer data is often compared to plutonium — powerful and valuable but terribly dangerous to the handler if abused," said Mike Pedrick, Vice President of Cyber Security Consulting at Managed Security Services Provider Nuspire.[3] This signifies that while we have no law to serve as guidance between blockchain technology's use of data at the moment, we cannot overlook the (NDPA) *Nigeria Data Protection Act*.[4] This act serves a foundation to implementation and guidance of personal data, providing a frame work for the compliance of data in Nigeria.

From data subjects to data controllers to the data itself, it needs a special ball effect rule in the blockchain space. With this in mind, this article seeks to expound on the importance of the protection of data whilst bearing in mind the utility which the instrumentality of the blockchain technology serves in this light, in view of the Nigerian perspective through its local legislations such as the *Nigeria Data Protection Act,* 2023. As this article aims to bring these two unique worlds together and to achieve its utmost regard to data in blockchain technology without breach. This would require collaboration, research and the will to act but, it is possible and it can be done.

2. Understanding the Nigeria Data Protection Act, 2023

The *Nigeria Data Protection Act, 2023* (here after referred to as "the NDPA") is the most recent law on data protection in Nigeria. It is also the primary legislation governing the processing of personal data as the Act takes priority over any other law or enactment relating directly or indirectly to the processing of personal data.[5] The Act commenced on the 12th of June 2023 upon being enacted by the National Assembly of the Federal Republic of Nigeria. The Act is said to have been enacted to provide a legal framework for the protection of personal information, and establish *the Nigeria Data Protection Commission (NDPC)* for the regulation of the

[1] TechBehemoths, 'Blockchain Companies in Nigeria'. https://techbehemoths.com/companies/blockchain/nigeria accessed 29 May 2024.

[2] National Information Technology Development Agency, 'Draft National Blockchain Adoption Strategy' (2020). https://nitda.gov.ng/wp-content/uploads/2020/10/DRAFT-NATIONAL-BLOCKCHAIN-ADOPTION-STRATEGY.pdf accessed 29 May 2024.

[3] TechTarget, 'Data Protection'. https://www.techtarget.com/searchdatabackup/definition/data-protection accessed 29 May 2024.

[4] Nigeria Data Protection Commission, 'Nigeria Data Protection Act 2023'. https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf accessed 29 May 2024.

[5] Nigeria Data Protection Act 2023, s63.

processing of personal information and for related matters. One of the primary objectives of the NDPA is to "strengthen the legal foundations of the national digital economy and guarantee the participation of Nigeria in the regional and global economies through the beneficial and trusted use of personal data."[6] The Act applies to both data controllers and data processors domiciled, resident, and operating in Nigeria as well as data controllers and data processors not domiciled in, resident, or operating in Nigeria, but processing personal data of a data subject in Nigeria.[7]

A Data Controller is an organization or individual who determines the purposes and means for processing personal data. They have the ultimate control over the data and are primarily responsible for ensuring compliance with the NDPA. Examples of Data Controllers include companies collecting customer data, social media platforms managing user information, or government agencies handling citizen data. A Data processor is an organization or individual who processes personal data on behalf of a Data Controller. They act according to instructions from the Data Controller and have specific obligations under the NDPA. The Data Controller gives instructions for processing to the data processor. The Data Processor cannot process personal data except upon the instructions of the controller. If a processor unlawfully processes personal data without instructions, they may be considered a controller instead. Processing involves any operation performed on personal data, such as, but not limited to, collection, structuring, storage, use or disclosure.[8] Examples of Data Processors include cloud storage providers storing customer data for a company, marketing agencies handling customer lists for targeted campaigns, or payroll processing companies managing employee data. *Section 3* of the NDPA provides that a guidance notice may be issued by the *Nigeria Data Protection Commission (NDPC)* containing legal safeguards and best practices to a data controller or processor. Data controllers and Data processors are to be registered by the NDPC.[9] The NDPC is also to ensure compliance with national and international personal data protection obligations and best practice.[10]

Section 24 of the NDPA provides for the duties of a data controller or data processor. The section provides that a data controller or data processor shall ensure that personal data is processed in a fair, lawful and transparent manner, collected for specified, explicit, and legitimate purposes, retained for not longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed, processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing, access, loss, destruction, damage, or any form of data breach, etc.[11] The section also provides that a data controller or data processor owes a duty of care, in respect of data processing.[12] It also provides that a data controller and data processor shall use appropriate technical and organizational measures to ensure confidentiality, integrity, and availability of personal data.[13]

Section 25 provides for the principles governing the legal processing of personal data. Consent from the data subject (that is, the person whose information is being collected, used and processed) is essential for the lawful processing of the subject's personal data.[14] The data subject should be informed of the right to withdraw consent, prior to the granting of consent. However, the withdrawal of consent will not affect the lawfulness of data processing that occurred before the withdrawal of the consent. The Act also stipulates that the request for consent shall be in clear and simple language and accessible format. A data subject shall have the right to withdraw consent at any time, and the data controller shall ensure that it is as easy for the

[6] Nigeria Data Protection Act 2023, s1(1)(h).

[7] Nigeria Data Protection Act 2023, s2(2).

[8] Clarip, 'Differences between a GDPR Data Controller vs. Data Processor'. https://www.clarip.com/data-privacy/gdpr-data-controller-vs-processor-differences/#:~:text=A%20data%20controller%20determines%20the,storage%2C%20use%20or%20disclosure accessed 29 May 2024. See also Nigeria Data Protection Act 2023, s 29. on the obligations of a data controller and data processor.

[9] Section 5 (d), 44.

[10] Section 5 (i).

[11] Section 24 (1) (a)–(f).

[12] Section 24 (3).

[13] Section 24 (2).

[14] Section 25 (1) (a) (b)(i)-(v).

data subject to withdraw, as to give consent.[15] Silence or inactivity of the data subject shall not constitute consent.[16]

The Act contains various other provisions on how data should be collected from individuals and the steps to be taken before the collection and processing of personal data.[17] *Part IV* of the Act provides for the rights of individuals whose data are being collected and processed by data controllers and processors.[18] *Part VII* says that a data controller and data processor shall implement technical and organizational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control. However whenever there is a breach of personal information, the data controller must report of the NDPC within 72 hours if it involves high risk and take proper measures to address and mitigate the harmful effects of the breach. *Part VIII* provides for the basis and guidelines for the transfer of personal data outside Nigeria.

The Nigerian Data Protection Act (NDPA) 2023 and blockchain technology pose a unique challenge. The NDPA focuses on giving control to data subjects over their personal data, while blockchain is designed to be secure and tamper-proof, with data potentially distributed across a network. Blockchain technology is often decentralized, meaning there's no single entity controlling the network. This makes it difficult to identify a clear Data Controller accountable under the NDPA. Data stored on a blockchain is typically immutable, meaning it cannot be easily altered or deleted. This clashes with the *Section 34 of the NDPA* which provides for data subjects to request erasure of their personal data without undue delay.

In most cases, data is collected by a central entity like a company or organization that stores it on their servers. This data can usually be modified or deleted by the entity that collected it. However, blockchain data collection is different, blockchain data isn't stored in one place but distributed across a network of computers. This makes it tamper-proof and very secure. Once data is added to a blockchain, it's generally very difficult or impossible to alter or delete it. Nevertheless, an important point to note is that while the data itself might be stored securely on the blockchain, the way it's used and interpreted depends on the applications or services built around the blockchain. These applications might collect additional data and should comply with relevant data protection regulations like the NDPA. The *Nigeria Data Protection Commission (NDPC)* is likely to issue specific guidance on how the NDPA applies to blockchain technology. This will provide clarity for organizations seeking to leverage blockchain while complying with data protection regulations.

3. Blockchain and Data Protection by Design

The concept "data protection by design" refers to the approach that integrates privacy and data protection considerations into the development of Information and Communication Technologies (ICTs) and organizational practices from the outset. This proactive strategy ensures that legal requirements, values, and principles are embedded within technological and business frameworks to safeguard personal data effectively.

In the context of blockchain technology, embracing the principles of data protection by design is essential. Currently, Nigeria lacks specific regulatory legislation addressing this aspect. Therefore, it is prudent to refer to international frameworks and best practices, such as the GDPR, as benchmarks. However, it is crucial to adapt these foreign standards to align with the unique legal and operational context in Nigeria.

The General Data Protection Regulation (GDPR) is a comprehensive data protection law enacted by the European Union (EU) and the European Economic Area (EEA) to protect individuals' personal data and privacy. It came into effect on May 25, 2018, and applies to all organizations that process the personal data of individuals within the EU and EEA, regardless of where the organization is located. It emphasizes the importance of incorporating "appropriate technical and organizational measures" during both the design phase and implementation of data processing activities to ensure compliance and protect the rights of data subjects (Art. 25(1) GDPR). This mandate implies that data protection considerations should be integrated

[15] Section 35 (1) (2).

[16] Section 26 (3). See also Section 31 on the NDPA's provision for children or persons lacking the legal capacity to consent.

[17] Section 27, 28 & 30.

[18] These individuals are collectively called Data Subject by the NDPA. See, Section 34–38, NDPA 2023.

into the design process well before the deployment of any data processing system. Failing to do so may result in non-compliance with the data protection by design principle and expose organizations to increased risks.[19]

In practical terms, incorporating data protection from the design stage enables blockchain technology to address several challenging compliance issues stipulated by the GDPR.

These include the roles and responsibilities of data controllers, processors, and joint controllers; ensuring data minimization and accuracy; managing data retention; and upholding data subject rights such as rectification and erasure (the right to be forgotten).

It is noteworthy that the data subject rights outlined in Section 34 of the Nigerian Data Protection Act (NDPA) are akin to those specified in Article 25 of the GDPR, reflecting a parallel commitment to data protection principles.

3.1. Possible Ways to Ensure GDPR (NDPR) Compliance in Blockchain Systems

This section outlines various strategies that can be adopted to ensure compliance with the General Data Protection Regulation (GDPR) and its Nigerian counterpart, the Nigeria Data Protection Regulation (NDPR). To facilitate this discussion, three common scenarios are defined based on how a data subject interacts with a blockchain. For each scenario, possible role assignments are proposed, along with strategies for data minimization and ensuring the right to erasure and amendment.

These scenarios are inspired by the categorization of blockchain systems, distinguishing between blockchains developed for specific purposes—either to store personal data or to process non-personal data—and non-specialized blockchains that can handle any type of data, similar to Smart Contract Platforms.

Scenario 1: Direct Interaction with a Permissionless Blockchain

In this scenario, an individual interacts directly with a permissionless blockchain, such as by buying and exchanging crypto currency without third-party intervention. The primary challenge here is the absence of a clearly identifiable data controller, making it difficult to hold anyone accountable for GDPR compliance. Consequently, the responsibility for compliance may fall on the users themselves, enforced through terms of use that:

- Prohibit the posting of certain types of personal data.
- Require users to obtain consent or have another legal basis for processing personal data.

Developers of permissionless blockchains may consider implementing techniques like zero-knowledge proofs to provide partial privacy guarantees. However, it is essential to recognize that depending on the blockchain's governance scheme, changes that reduce compliance might be introduced.

Scenario 2: Applications Using Permissionless Blockchains as a Backend

In this scenario, a data subject interacts with an application that uses a permissionless blockchain as a backend, such as Ethereum Smart Contracts. Here, the application's owners can be identified as data controllers because they determine what personal data is collected and how it is stored and processed on the blockchain. They are responsible for informing users that some of their personal data will be stored on a blockchain and for implementing strategies to hash, encrypt, and protect this data.

To ensure GDPR compliance, personal data should be hashed before being stored on a server controlled by an identifiable data controller. To reduce the risk of pre-image attacks, advanced salting techniques can be employed, where a random string (salt) is concatenated to the data before encryption. Additionally, any table that matches pseudonyms (e.g., public keys) generated for data subjects with their identities must be stored off-blockchain. In cases where processing personal data is encoded in a smart contract and hashing is not feasible, multi-party private computation schemes may be an option. However, further research is required to verify that these schemes offer the necessary level of decentralization.

[19] GDPR-Info.eu, 'Privacy by Design'. https://gdpr-info.eu/issues/privacy-by-design/ accessed 29 May 2024.

Scenario 3: Permissioned Blockchains

This scenario is further divided into two sub-cases:

1. Individual Participation in a Permissioned Blockchain Consortium: In this sub-case, an individual voluntarily joins a consortium to run a permissioned blockchain. The individual must acknowledge that others may process any data they input and that they are responsible for validating transactions, which comes with associated responsibilities in the event of a data breach or misuse. A possible role assignment is that all consortium members are joint data controllers. They must agree on how to handle requests related to GDPR rights.

2. Permissioned Blockchain Consortium Offering Services to End-Users: In this sub-case, the consortium offers services to end-users, storing their personal data on the blockchain. To ensure compliance, consortium members should declare themselves joint data controllers. The most effective approach to compliance involves the use of common sense and adherence to established data protection practices.

Checklist for Blockchain Data Processors

To ensure GDPR compliance, data processors using blockchain technology should address the following questions:

1. What personal data will be collected, and what portion will be stored or processed on the blockchain?

2. What processing will the personal data undergo on the blockchain, and what are the advantages of decentralizing this process?

3. What type of blockchain will be used, and what is known about the validators? Can they be bound by a contractual agreement?

4. If data is encrypted or hashed before entering the blockchain, who holds the encryption keys or links to the original data?

Permissioned Blockchain Compliance Strategies

Permissioned blockchains rely on cryptographic techniques, such as encryption and pseudonymous identities, to comply with GDPR requirements. Pseudonyms help ensure the unlinkability of transactions and user anonymity, while encryption ensures that only authorized parties can access transaction data. Permissioned blockchains, like Hyperledger Fabric (HLF), offer access control mechanisms that further protect user data. HLF also utilizes advanced cryptographic techniques, such as Zero-Knowledge Proofs (ZKPs), which allow for proof generation without revealing the underlying data. The immutable nature of blockchains guarantees data integrity, making permissioned blockchain models well-suited to meet GDPR requirements for data controllers.

By integrating these strategies into blockchain design and operations, organizations can achieve compliance with GDPR and NDPR mandates, safeguarding the privacy and rights of data subjects.

4. NDPA Provisions Relevant to Blockchain

Section 33 of NDPA states *"The Commission may license a person having a requisite level of expertise, in relation to data protection and this Act, to monitor, audit and report on compliance by data controllers and data processors…"* this implies that for every privacy or blockchain compliance officer. Such person must be licensed by the Nigeria data privacy authority before he carries out any operation. In the future, there should be a report system in place to track its formality.

The right of a data subject as stated in *Section 33 of the NDPA* should not be left out while building a blockchain. This would best fit a private blockchain. One of the advantages of using a blockchain technology is its anonymity however, it can be traced in the space. This raises the question of due diligence to ensure the right information is being stored. What of if a slight negligence occurs in giving a wrong data? Who bears the loss? What happens to the victim?

For public blockchain, a system needs to be built to ensure these codes which are individual data are kept safe from unsolicited services. Although we do not have a law guiding blockchain in Nigeria, the National blockchain policy 2023 serves a roadmap, a foundation for the acceptance of blockchain technology in Nigeria and subsequently, more guided guide path would be established to regulate this industry.

Since blockchain cannot be restricted all over the world, a privacy specialist can help assist the government in passing regulations for data privacy in blockchain technologies. Thus in relation with cross data transfer in blockchain technology affecting the privacy space, regulations should be put in place to enable the smooth flow and avoid abuses. In the future we might have several conflicts with various technologies building on the blockchain of this is not resolved. I also call on privacy specialist to help the government. It is usual that the law is racing after innovation but it would be sad if we do nothing at all.

5. Best Practices for Implementing Data Protection by Design in Blockchain

Data Protection by Design (DPbD) is an approach to data protection that involves integrating data protection principles and safeguards into the design and development of systems, processes, and products. It aims to ensure that data protection is considered from the outset, rather than as an afterthought. By incorporating DPbD into their systems, processes, and products, organizations can demonstrate their commitment to data protection and privacy, and help to ensure the security and integrity of personal data. DPbD is required by the General Data Protection Regulation (GDPR) and is considered a best practice for organizations that process personal data.[20] It helps organizations to perform functions such as building trust with customers and users, complying with data protection regulations, reducing risks of data breaches and cyber-attacks, improving data security and privacy, enhancing their reputation and brand and so many other functions.

However, implementing data protection by design in blockchain technology requires a thoughtful and multi-layered approach. There are best practices to consider and they include; First, conducting a Data Protection Impact Assessment (DPIA) which entails identifying potential data protection risks and opportunities for mitigation. Second, Implementation of privacy by design and default and this means Incorporating data protection principles and safeguards into the design and development of blockchain systems.[21] Another best practice is using encryption and hashing and this has to do with protecting personal data using end-to-end encryption and hashing techniques and this will enable transparency and accountability: To respect data subject rights, mechanisms for data subjects to exercise their rights, such as access, correction, and deletion can also be implemented.

Ensuring data minimization and purpose limitation entails collecting and processing only necessary personal data for specified purposes. A data subject should not be required to give out more information than necessary. Also, implementing data protection by design for smart contracts and incorporating data protection principles into smart contract design and development is another best practice. Using decentralized identity management systems to protect personal data and enable user control and fostering a culture of data protection by educating and training developers, users, and stakeholders on data protection are other best practices.

By implementing these best practices, blockchain technology can effectively protect personal data and maintain trust in the decentralized ecosystem. These best practices are not exhaustive and may evolve as blockchain technology and data protection regulations continue to develop.

6. Case Studies and Examples

Bitcoin is an online cash currency launched in early 2009. Bitcoin was created to be a form of electronic cash that could be sent peer-to-peer without the need for a central bank or other authority to operate and maintain the ledger, much as how physical cash is used. The engine that runs the bitcoin ledger is original and largest blockchain, while other blockchains run several hundred other similar currency projects with different rules.

[20] FasterCapital, 'ICO Privacy: Data Protection in Blockchain & ICO Best Practices'. https://fastercapital.com/content/ICO-privacy—Data-Protection-in-Blockchain—ICO-Best-Practices.html accessed 29 May 2024.

[21] Kerstin Lemke-Rust and others, 'Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data' (2018). https://www.researchgate.net/publication/326246922_Privacy_by_BlockChain_Design_A_Blockchain-enabled_GDPR-compliant_Approach_for_Handling_Personal_Data accessed 29 May 2024.

Smart contract is another example and it allows for transactions to be made automatically and without the need to rely on a central party to adjudicate the operation of the contract terms. Blockchain offers opportunities in this arena, because smart contract code can be written directly onto a block and is examinable by the contracting parties ahead of time, just like a traditional legal contract. If it is agreed to, then the smart contract will automatically execute its own terms. This could mean releasing a payment following a certain trigger, running a software escrow account or making an investment.

Blockchains are designed to be useful in systems that require reconciliation between parties. Many of the major players in banking are backing the R3 consortium, which is researching the use of a blockchain-like distributed ledger for interbank reconciliations and other financial applications.

However, successful implementation of Data Protection by Design (DPbD) in Nigeria can be seen in various initiatives and organizations, including: The National Identity Management Commission (NIMC) which implemented a privacy-by-design approach for the national identity database, ensuring the protection of citizens' personal data. The Central Bank of Nigeria (CBN) also Incorporated DPbD principles into its digital payment systems, safeguarding financial data and promoting trust in the financial sector.

The Nigerian Communications Commission (NCC) adopted DPbD in its data protection guidelines for telecom operators, ensuring the privacy and security of subscribers' data. There have also been many e-government initiatives many Nigerian government agencies have implemented DPbD in their online services, protecting citizens' personal data and promoting transparency.

Also, private sector organizations like Andela, Flutterwave, and Kuda Bank have integrated DPbD into their systems, demonstrating a commitment to data protection and privacy. These examples demonstrate Nigeria's progress in implementing DPbD, ensuring the responsible handling of personal data and promoting trust in various sectors.[22]

7. Conclusion

The intersection of blockchain technology and data protection by design (DPbD) is a crucial area of exploration, particularly in the context of the Nigerian Data Protection Act (NDPA). The NDPA's provisions and best practices offer a robust framework for ensuring the responsible handling of personal data in blockchain applications. DPbD is an essential approach in blockchain development, as it integrates data protection principles and safeguards into the design and development of systems, processes, and products. By adopting DPbD, blockchain developers can ensure that data protection is prioritized from the outset, rather than as an afterthought.

The NDPA's provisions offer a comprehensive framework for data protection in Nigeria, and its best practices provide guidance on implementing DPbD in blockchain applications.

By embracing DPbD and the NDPA's provisions, blockchain developers can create trustworthy and secure applications that prioritize users' data privacy and security. As blockchain technology continues to evolve, it is crucial to prioritize data protection and privacy, and the NDPA's provisions and best practices offer a valuable guide for achieving this goal.

In the words of the National Data Protection Commission (NDPC), "*Data protection is a fundamental right, and it is our collective responsibility to ensure that this right is respected and protected.*"[23] By adopting DPbD and the NDPA's provisions, we can build a trustworthy and secure digital ecosystem that prioritizes users' data privacy and security.

References

Clutch. (2024). Top Blockchain Developers in Nigeria. https://clutch.co/ng/developers/blockchain

FasterCapital. (2024). ICO Privacy: Data Protection in Blockchain & ICO Best Practices. <https://fastercapital.com/content/ICO-privacy—Data-Protection-in-Blockchain— ICO-Best-Practices.html>

[22] Clutch, 'Top Blockchain Developers in Nigeria'. https://clutch.co/ng/developers/blockchain accessed 29 May 2024.

[23] Nigeria Data Protection Commission, 'Privacy Policy'. https://ndpc.gov.ng/Home/Privacy accessed 29 May 2024.

GDPR-Info.eu. (2024). Privacy by Design. https://gdpr-info.eu/issues/privacy-by-design/

Kerstin Lemke-Rust. (2024). Privacy by Blockchain Design: A Blockchain-Enabled GDPR-Compliant Approach for Handling Personal Data. https://www.researchgate.net/publication/326246922_Privacy_by_BlockChain_Design_A_Blockchain-enabled_GDPR-compliant_Approach_for_Handling_Personal_Data

National Information Technology Development Agency. (2020). Draft National Blockchain Adoption Strategy. https://nitda.gov.ng/wp-content/uploads/2020/10/DRAFT-NATIONAL-BLOCKCHAIN-ADOPTION-STRATEGY.pdf

Nigeria Data Protection Act. (2023). Clarip, Differences between a GDPR Data Controller vs. Data Processor. https://www.clarip.com/dataprivacy/gdpr-data-controller-vs-processor-differences/#:~:text=A%20data%20controller%20determines%20the,storage%2C%20use%20or%20disclosure

Nigeria Data Protection Commission. (2023). Nigeria Data Protection Act 2023. https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf

Nigeria Data Protection Commission. (2024). Privacy Policy. https://ndpc.gov.ng/Home/Privacy

TechBehemoths. (2024). Blockchain Companies in Nigeria. https://techbehemoths.com/companies/blockchain/nigeria

TechTarget. (2024). Data Protection. https://www.techtarget.com/searchdatabackup/definition/data-protection

Cite this article as: Elesho Oluwabukolami Morenike, Grace Ihinosen Akhihiero, Okhiai Elizabeth Blessing, Mobolaji Oyelola Bankole, Adesuyi Omobolanle Blessing and Adebayo Adetayo Elizabeth (2024). Blockchain and Data Protection by Design: An Examination of The Ndpa's Provisions and Best Practices. *International Journal of Cryptocurrency Research*, 4(2), 126-134. doi: 10.51483/IJCCR.4.2.2024.126-134.