

CHAPTER 4 – RESULT AND DISCUSSIONS

This chapter presents the findings of the research and analyzes them in relation to the study's objectives and theoretical framework. The results are organized to address the research questions, with a discussion highlighting key insights, implications, and contributions to theory and practice. Challenges and limitations encountered during the study are also addressed.

4.1 Blockchain, PDP Law, HARA Agriculture Data Gap Analysis

This section presents a comprehensive gap analysis conducted to evaluate the current state of HARA's agricultural data in relation to the compliance requirements of the PDP Law using blockchain technology. The analysis aimed to identify discrepancies between existing blockchain data practices and the regulatory standards outlined in the PDP Law to address RO1. The insights gained from this gap analysis provide the foundation for the initial design proposed in this study to achieve RO2.

Table 4.8 illustrates the gap analysis conducted on HARA's data regarding the PDP Law. This analysis aims to identify and address the discrepancies between the current state and the desired state required for compliance. Each component highlights key aspects of the PDP Law and their relevance to the thesis. The table specifies the identified gaps, which serve as the baseline for solution design and provide valuable feedback for improving the application.

The high relevance to the thesis will be reflected in the focus on updating the solution. For example, in the "Data Subject Rights" component, it was identified that the right to erasure is not currently supported, requiring a different approach for data recorded on the blockchain. This aligns with the theory discussed (Godyn et al., 2022), which addresses the challenges associated with blockchain technology and data privacy. These findings underscore the complexities of ensuring compliance with data protection laws in blockchain-based systems and will guide the development of more effective solutions.

Table 4.8. Gap Analysis in HARA Based on PDP Law.

No	PDP Law Component	Relevance	Current State	Desired State	Gap Identified
1	Data Collection and Consent	Medium	- The consent clearly outlines the purpose of data processing and provides detailed information about each program that will utilize the personal data. - A mechanism for consent withdrawal has not yet been implemented within the application.	- The purpose of data collection is clearly and transparently communicated to data subjects within the consent process. - A straightforward mechanism is in place to allow data subjects to withdraw their consent at any time.	No consent withdrawal mechanism implemented. Need to establish an easy-to-use system for consent withdrawal.
2	Data Processing and Use	Medium	- Personal data is used for farmer or agent verification and program purposes, such as loans or insurance. - Not all lawful bases for data processing have been thoroughly reviewed by the legal team.	- Data use with limitation that specified. - Lawful basis for each processing reviewed.	Lack of review for all lawful bases of data processing. Ensure all data processing activities are clearly linked to legal grounds.
3	Data Security and Protection	High	- Data is encrypted using AES-256 in both the database and the blockchain. - Each role is assigned specific permissions to access data within the data acquisition application. - Personal data is displayed using masking techniques to protect sensitive information.	- Robust security measures in place, including encryption and access controls.	Adequate encryption and role-based access exist, but further strengthening of security policies and controls may be needed.

Table 4.9. Gap Analysis in HARA Based on PDP Law (cont.).

No	PDP Law Component	Relevance	Current State	Desired State	Gap Identified
4	Data Retention and Disposal	High	- No retention period has been defined yet for personal data. - Permanent deletion is not fully achievable in blockchain transaction history, even when data is remove from the smart contract.	- Personal data should only be retained for as long as necessary for its stated purpose. - Review procedures for secure and timely disposal of data no longer required.	No defined retention period. Need to establish clear retention policies and address blockchain's immutability for data deletion.
5	Data Subject Rights	High	- All right covered except the right to erasure, because the transaction history is immutable.	Ensure each individual allow to have: - Right to access their data. - Right to correct inaccurate data. - Right to erasure ("right to be forgotten"). - Right to data portability. - Right to restrict or object to processing.	Right to erasure is not achievable due to immutability of blockchain. Alternative methods need to be implemented to address this.
6	Third-Party Management	High	- Third-party data sharing is acknowledged and consented to by the data subject. - Certain data is collected by agents, who are granted access to view the farmer's personal data.	- Third parties comply with PDP Law requirements and are regularly audited.	Lack of regular auditing for third-party compliance. Ensure third-party compliance with PDP Law through regular audits.
7	Training and Awareness	Low	- No regular training programs are conducted. - Only two awareness events were held during the initial implementation phase for employees.	- Regular training programs for employees on PDP Law compliance.	Absence of continuous training. Implement periodic training programs for all employees.

In conclusion, based on gap analysis in Table 4.8 confirms that aligning HARA's blockchain-based data management practices with the PDP Law requires significant changes. RQ1 is addressed through the identification of structural modifications required for compliance, while RQ2 is answered by validating that a hybrid approach is the most effective solution. Furthermore, H1 is confirmed, as various compliance gaps indicate that the PDP Law necessitates revisions in HARA's data.

By addressing these challenges, the study lays the foundation for PrivAgri, a privacy-preserving framework designed to achieve PDP Law compliance while optimizing HARA's data acquisition product. This framework ensures that on-chain records remain immutable but unlikable to personal data, while off-chain storage provides flexibility for regulatory compliance.

4.2 Developing Solution Design to Comply PDP Law

Article 27 of the PDP Law mandates that data controllers collect only the personal data that is directly relevant and necessary for a specified purpose. This principle requires minimizing data collection to align with its intended use. By applying data minimization, HARA ensures that only essential variables are recorded, reducing unnecessary data storage and enhancing compliance. This approach serves as a key strategy in achieving RO2 by addressing RQ2.

Table 4.10 outlines the variables that should or should not be collected, with the status column indicating whether a variable is required based on its specific purpose.

Table 4.10. Minimization Applied in HARA Acquisition Application Structure.

Type of Data	Data	Status	Purpose	Notes
Farmer's Data	Full Name	Y	Farmer Validation	
	Phone Number	Y	Farmer Validation	
	Citizen Identity Number	Y	Farmer Validation	
	Name of <i>Kelompok Tani</i>	Y	Farmer Validation	
	Regency/City	Y	Farmer Validation	
	District	Y	Farmer Validation	
	Subdistrict/Village	Y	Farmer Validation	
	Residence Address	Y	Farmer Validation	
	E-STDB Document	N	Government Validation	Temporarily for validation and delete immediately after validation by the government service.
	<i>Kartu Tani</i> Photo (<i>Kartu Tani ID</i> and full name)	N	Government Validation	Temporarily for validation and delete immediately after validation by the government service.
	Farmer Status	Y	Flag for Validation	

Table 4.11. Minimization Applied in HARA Acquisition Application Structure
(cont.).

Type of Data	Data	Status	Purpose	Notes
Land Data	Land Name	N		
	Land Area	Y	Land Validation	
	Land Coordinate	Y	Land Validation	
	Land Polygon	Y	Land Validation	
	Province	Y	Land Validation	
	Regency/City	Y	Land Validation	
	District	Y	Land Validation	
	Subdistrict/Village	Y	Land Validation	
	Plan Variety	Y	Land Validation	
Loan Data	Bank Name	Y	Transaction for Loan Registration	
	Number of Saving	Y	Transaction for Loan Registration	
	Estimated Planting Date	Y	Transaction for Loan Registration	
	Photo of Agreement Document	Y	Transaction for Loan Registration	
	Farmer's Selfie with Agreement Document	Y	Transaction for Loan Registration	

Based on the outlined conditions, a framework called PrivAgri has been introduced to fulfill RQ2 in achieving RO2. PrivAgri consists of four modules designed to ensure full compliance with the Personal Data Protection (PDP) law. These modules address key aspects of data management, offering a comprehensive approach to securely and efficiently handling personal data.

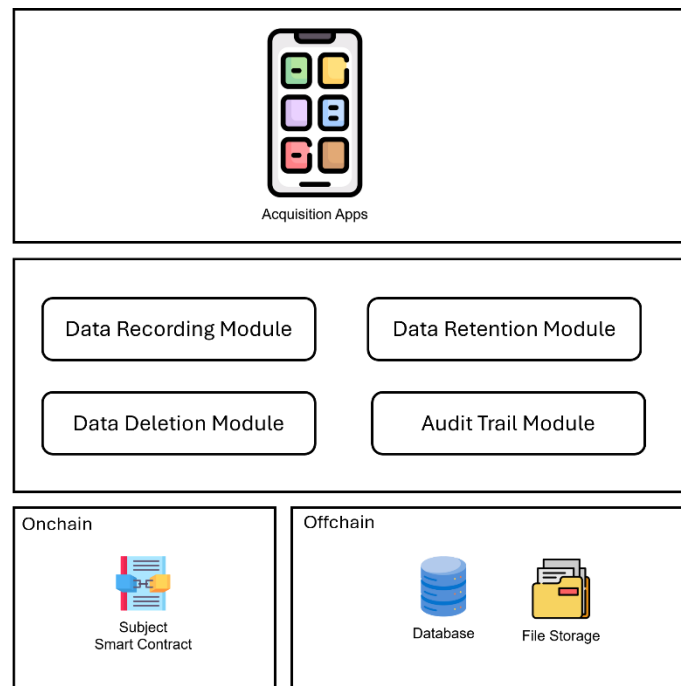


Figure 4.11. PrivAgri, Proposed Solution in HARA Acquisition Application

As seen in Figure 4.11, these modules including:

- **Data Recording Module:** This module ensures that all personal data is accurately and systematically recorded in a secure manner, adhering to standardized processes and protocols.
- **Data Deletion Module:** This module governs the secure and irreversible deletion of personal data once it is no longer required, ensuring compliance with the PDP law's provisions on data lifecycle management. It also mitigates risks related to other legal compliance in Indonesia.
- **Data Retention Module:** Designed to regulate how long personal data is stored, this module complies with the PDP law requirements for data retention periods. It prevents unnecessary storage of data while maintaining accessibility for operational and legal purposes.
- **Audit Trail Module:** logs all activities related to data subjects, ensuring immutable and transparent to data subject.

Considering the literature on chapter 2.2.2 the solution adopts both on-chain and off-chain approaches. The on-chain component utilizes smart contracts to record subject-related data in encrypted form. Meanwhile, the off-chain infrastructure leverages a cloud provider that supports the Indonesia region. The databases store personal data

and manage encryption keys to ensure data protection before linking to the smart contract. Additionally, a file storage is used to store subject-related files within the ecosystem.

4.2.1. Recording Module

The Recording Module outlines the entire flow of data from the point of entry through the HARA acquisition applications to its subsequent recording in both blockchain (on-chain) and data storage systems (off-chain). The module ensures that this data is securely recorded on the blockchain, providing an immutable and transparent record that is stored on-chain. Simultaneously, the module also manages the storage of relevant data off-chain, where it can be accessed and used for operational purposes without compromising the integrity of the on-chain data. This dual storage system ensures that the data is both archived and readily accessible, while maintaining compliance with relevant data protection laws and providing flexibility for different use cases.

A subject smart contract is a smart contract that records the entities data including farmer and land. The key components include:

1. State variables: identifier of subject (subjectId), struct of subject information (subjectInfo), version mapping of subject (subjectVersion), status of subject (subjectStatus)
2. Functions
 - a. addSubject(): Adds new subject data by recording essential information on the blockchain.
 - b. getSubject(): Retrieve subject information that recorded in smart contract based on subject id and version.
 - c. updateSubject(): Update subject information with incrementing the version to maintain version control.
 - d. deleteSubject: Flags a subject as inactive using a status variable
 - e. checkIntegrity(): Verifies the consistency of subject data, particularly for off-chain values, ensuring that both on-chain and off-chain data remain intact. This function helps confirm that the data has not been altered, corrupted, or tampered with, thereby maintaining the reliability and accuracy of the entire system.

- f. `sharingSubject()`: Logs any subject activity beyond basic actions such as add, update, or get. This function tracks specific interactions or data exchanges involving the subject, providing an audit trail of actions taken, particularly those related to external sharing or transfers of data.

3. Events

- a. Logs activity of a subject (SubjectActivities)

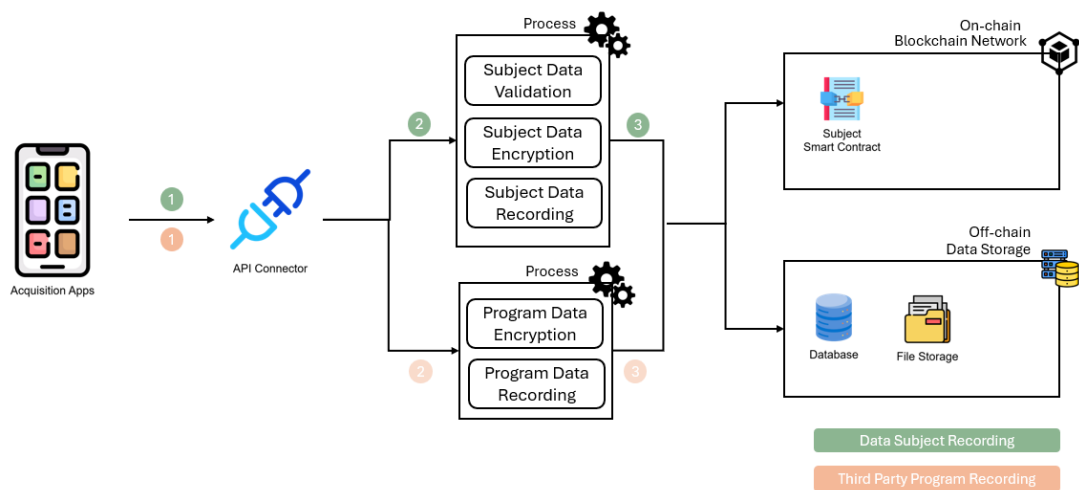


Figure 4.12. Recording Module Flow.

Figure 4.12 illustrates the flow of the recording module. This module consists of two flow, data subject recording and third-party program recoding (i.e. loan registration). The data subject recording is following:

1. A user of HARA inputs the data through the acquisition application. In the backend, this action triggers an API connector that processes the data input.
2. The inputted data is processed into three parts:
 - a. Subject data validation: This is a preprocessing step to validate the data, ensuring for no duplicates, unstandardized entries, and inconsistencies.
 - b. Subject data encryption: The data is encrypted using the AES-256 encryption algorithm. A unique key is generated for each user to guarantee the security and confidentiality of personal data.
 - c. Subject data recording: The validated and encrypted data is prepared for recording in both on-chain and off-chain storage systems. The blockchain automatically maintains an audit trail, capturing details such as recording activity, the address interacting with the smart contract, and timestamp information.

3. The encrypted data is recorded on the blockchain, ensuring data integrity using the SHA-256 hash algorithm. This guarantees that the data remains immutable. It is stored in the Subject Smart Contract deployed on the HARA ledger, while other related data and keys are recorded in a database and file storage system.

The distinction in program data recording depends on the type of data specific to each third-party program. For example, in loan registration, the recorded data includes variables required in the registration form, along with the data subject's agreement allowing data transfer to a third party for loan processing. This ensures that only necessary and permitted data is shared while maintaining compliance with PDP law.

In summary, the Recording Module securely processes data from input to storage, as shown in Figure 4.12. Data is validated to prevent inconsistencies, encrypted using AES-256, and recorded on both the blockchain and off-chain storage. The use of SHA-256 ensures data integrity, making it immutable and secure. This approach guarantees both privacy and data availability while maintaining a reliable framework for managing sensitive information

4.2.2. Deletion Module

The Data Deletion Module complies with Article 43 of the PDP Law, which grants data subjects the right to request data deletion when their personal data is no longer needed, has been processed unlawfully, or when consent is withdrawn. This provision aligns with the data subject rights outlined in Article 8, ensuring their right to terminate processing, delete, and/or eradicate their personal data in accordance with applicable laws and regulations. To ensure compliance, the module supports soft deletion, rendering the data inaccessible to users while retaining the data for potential legal or operational purposes.

However, considering article 15 of the PDP Law, which outlines exceptions to data subject rights, compliance must also adhere to POJK Number 39/POJK.05/2020 and UU No. 8 Tahun 1997. These regulations mandate specific retention periods and disposal practices for financial and archival data, requiring certain data to be retained

for a legally prescribed duration. This ensures a balance between data subject rights and regulatory obligations governing data retention and disposal.

The retention period is 10 years, as defined by UU No. 8 Tahun 1997, which aligns with and fulfils the retention requirements set by other related regulations. By integrating these legal requirements, the data deletion Module ensures lawful data disposal, upholds data subject rights, and adheres to sector-specific regulations, fostering accountability and trust in data management practices.

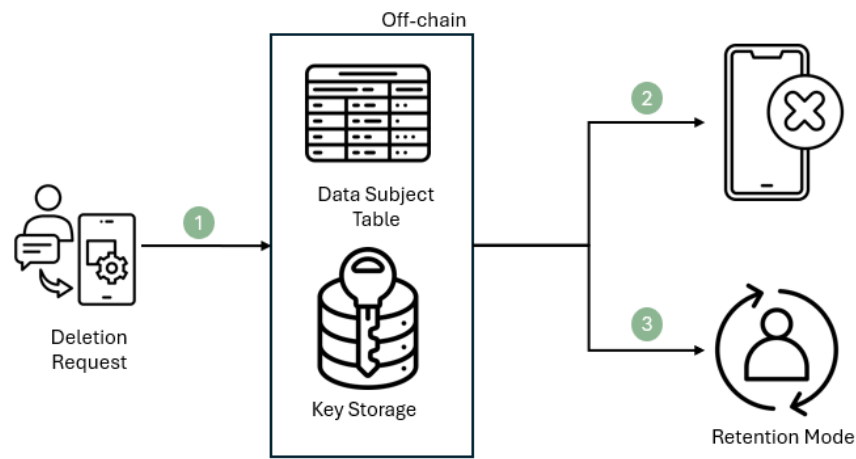


Figure 4.13. Deletion Module Flow

The Data Deletion Module primarily affect off-chain data storage, while on-chain data remains unchanged. The on-chain data remains in retention mode because blockchain's immutability prevents direct deletion. Instead of erasing on-chain records, the system flags the associated data off-chain as "is_deleted" and restricts access while preserving hashes or metadata on-chain. Figure 4.13 illustrates the flow of the data deletion process, starting from the initial request made by the user. The flow consists of the following steps:

1. User Request deletion will update the data subject table with is_deleted status with timestamp to capture the retention period. No action in key storage.
2. In application, the user is not found due to the flag of the is_deleted to comply PDP for data subject rights.
3. While the data remains to retain in the retention period to comply with POJK Nomor 39/POJK.05/2020 and UU No. 8 Tahun 1997

4.2.3. Retention Module

The Retention Module addresses two scenarios: permanent deletion and re-identification requests. Permanent deletion aligns with the definition of extermination stated in Article 44 of the PDP Law. By removing the key that links off-chain and on-chain data, it ensures that the data can no longer be associated with the data subject, fulfilling the legal definition of extermination. Re-identification requests are supported in accordance with Article 15, which outlines data subject rights, and Article 50, which defines the obligations of data controllers, allowing exceptions for legal and governmental purposes. When re-identification occurs, access is strictly limited to authorized users involved in legal or regulatory cooperation. Additionally, in compliance with POJK Nomor 39/POJK.05/2020 and UU No. 8 Tahun 1997, the module permits the retrieval of financial data under special circumstances, such as legal investigations or audits. The default retention period is set at 10 years, as mandated by UU No. 8 Tahun 1997, which prescribes the longest retention period among relevant regulations. However, for specific cases, certain data may be retained beyond this period to meet business, regulatory, or operational requirements.

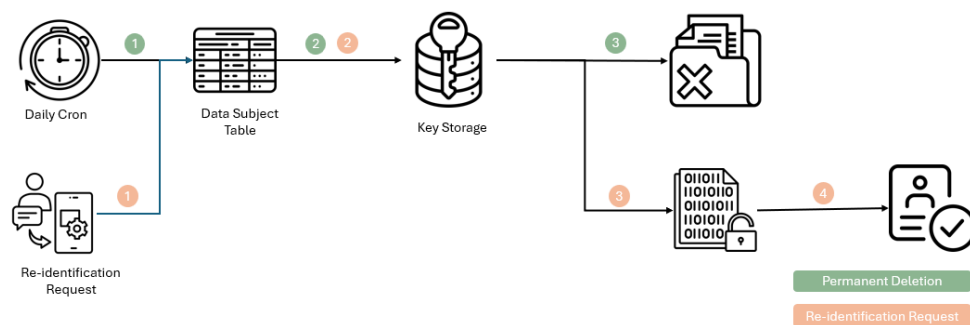


Figure 4.14. Retention Module Flow

Based on Figure 4.14, the steps for removing data subjects when the retention period is exceeded are as follows:

1. Daily cron job checks for any rows in the table that exceed the retention period.
2. For data that exceed retention, the encryption key and uuid salt removed from key storage.

- There is no longer any connection between off-chain and on-chain data. While the data in the smart contract remains, it is no longer linked to any data subject. The off-chain data is removed to comply with the deletion request. Figure 4.15 illustrates the data conditions before and after permanent deletion. The only remaining data is the on-chain record stored in the smart contract, but it cannot be linked to any identifiable information.

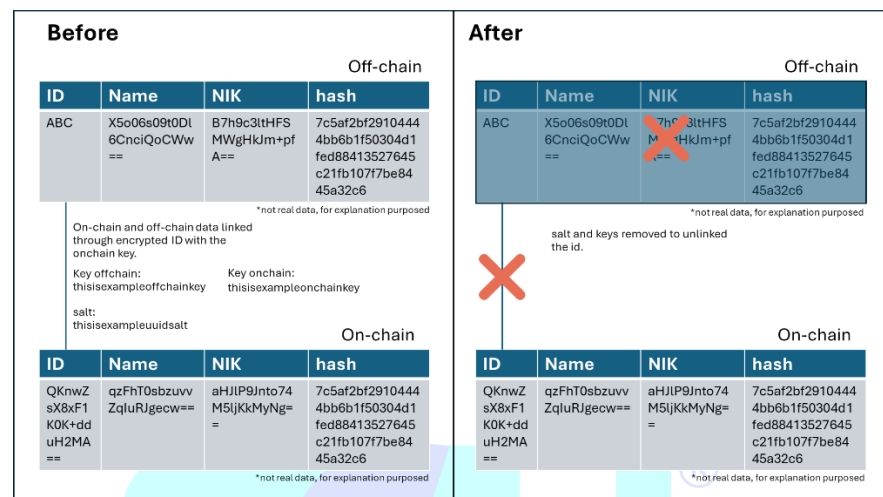


Figure 4.15. Permanent Deletion Example.

For re-identification requests, the steps are:

- The user submits a re-identification request for special circumstances.
- The requested data subject is checked to determine whether their data is still within the retention period. If the data is still under retention, the associated key and UUID are retrieved to re-identify the data subject.
- The decryption process is carried out using the retrieved keys.
- The data subject's information is successfully retrieved and made available for the specific request.

4.2.4. Audit Trail Module

In line with Article 27 of the PDP Law, the system ensures transparency by providing data subjects with clear visibility into how their personal data is processed and shared. All data access and processing activities are recorded on the blockchain (on-chain), ensuring immutability and preventing unauthorized modifications. This creates an

auditable log that allows data subjects to verify how their information is handled, reinforcing trust and compliance.

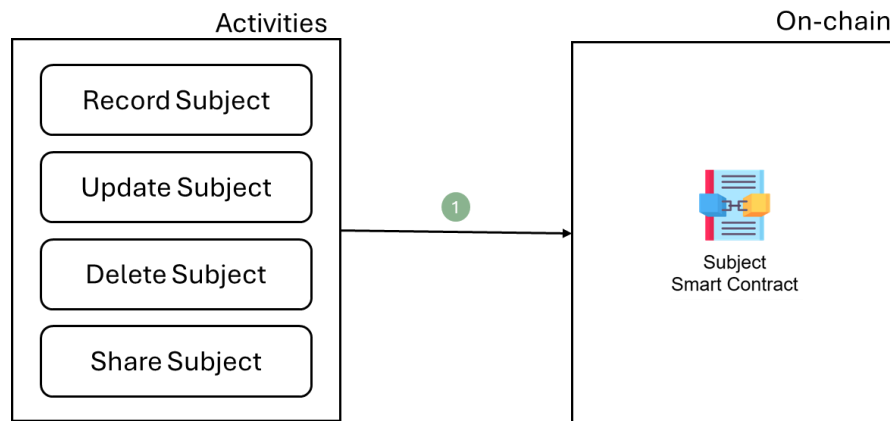


Figure 4.16. Audit Trail Flow.

Based on Figure 4.16, all activities related to the data subject are automatically logged, capturing activity details, timestamps, and the triggering smart contract address. This enables comprehensive tracking of interactions linked to a specific subject ID. The blockchain ensures these records remain immutable, preserving data integrity and preventing unauthorized modifications. By maintaining this record, data subjects can monitor how their data is used, enhancing transparency and control over their personal information.

4.3 Evaluation

The evaluation process aims to assess the effectiveness and compliance of the proposed data structure and management framework within HARA's data acquisition system, ensuring alignment with Indonesia's PDP Law. This evaluation in Table 4.12 will focus on Article 27, Article 43, and Article 44, which govern transparency, data deletion, and data extermination, respectively. This process is essential in answering RQ2, as it identifies and validates key strategies for designing compliant data structures within a blockchain-integrated system. The structured approach ensures that personal data is handled securely, aligning with PDP Law's regulatory mandates while maintaining blockchain's core advantages. The PrivAgri framework's hybrid model validates H2 by confirming that a hybrid data management framework is the optimal strategy for balancing privacy protection, regulatory compliance, and blockchain benefits.

Table 4.12. PDP law mapping with PrivAgri framework.

Legal Requirement	Component	Compliance Status	Notes
Article 27	- Data minimization applied - Blockchain-based audit trail	Yes	Ensures limited, specific, and transparent data processing.
Article 43	- Soft delete mechanism - Deletion request	Yes	Users can request deletion, with no visible data remaining in the app.
Article 44	- Off-chain deletion mechanism - Cryptographic key removal for unlikability	Yes	On-chain data is unlinkable from any specific data subject.

4.3 Validation

After defining the proposed solution design for the HARA acquisition application to ensure compliance with PDP law, the design will be validated by experts. The validation process will involve conducting interviews with blockchain and data privacy experts to gather their insights and feedback. The participation for the validation is as follows:

Name	Role	Expertise
Yos Ginting	Founder <i>Asosiasi Blockchain Indonesia</i>	Blockchain
Satriyo Wibowo	Data Privacy Consultant	Data Privacy

The feedback from users highlighted the comprehensiveness and relevance of the design, with specific recommendations for improvements.

1. Blockchain Expert

The role of blockchain in the HARA solution needs further clarification, particularly regarding its necessity and advantages. In the future, blockchain will play a crucial role in handling AI-driven transactions, as industries increasingly shift toward autonomous digital ecosystems. Its decentralized, transparent, and secure nature makes it ideal for managing data integrity and trust in automated systems. By integrating blockchain, HARA can enhance transaction security, ensure data immutability, and support the evolution of AI-powered decision-making processes in digital industries.

Each module needs to have a capability to face the future with the emerging fast technology improvement, especially in AI. The record module should add capabilities to distinguish between human and AI-initiated transactions,

2. Data Privacy Expert

The data privacy expert categorized the deletion process into two concepts deletion, as defined in Article 43 of the PDP Law, and extermination, as outlined in Article

44 (Presiden Republik Indonesia, 2022). Deletion refers to the removal of data from the user interface or application, ensuring that the data subject can no longer access or view the information. However, some traces of the data may still exist within the system. In contrast, extermination ensures that all references to the data subject are permanently removed, making it impossible to retrieve or associate the data with the individual. The proposed deletion module incorporates both concepts, ensuring compliance with PDP law practices.

If personal data is requested for essential processes like loan registration or insurance activation, the legal basis should be of contractual necessity rather than consent, as the data processing is required to fulfill an agreement. To address this, the consent module should be revised to explicitly recognize contractual basis as a valid legal basis, ensuring that data processing for such purposes is clearly defined and properly regulated. This revision should also include safeguards to prevent misuse, ensuring that only the necessary data is processed and that data subjects remain informed of their rights under the PDP Law.

Based on the feedback, the proposed solution design emphasizes the crucial role of blockchain integration in the system. Each module is enhanced to seamlessly incorporate blockchain. The challenges posed by AI-driven processes will require further research as they are outside the current scope. Notably, the consent module has been restructured into an audit trail module, ensuring immutability and transparency of activities to support contractual legal bases and all data subject-related activities. This transformation promotes regulatory compliance, tamper-proof logging, and the system's adaptability to evolving technologies and PDP law requirements.

The proposed design has been shared with HARA's stakeholder as input to enhance the current ecosystem and ensure compliance with the PDP law. This serves as a foundational step for improving HARA's data management with blockchain. By incorporating these inputs, the ecosystem will be further aligned with legal requirements, enabling continuous adaptation to emerging regulatory standards and fostering a robust approach to data protection and privacy.