Data Protection Impact Assessment Framework in the Banking Sector in Indonesia to Implement Law of Personal Data Protection

Dian Ismiati Anggraini*
Faculty of Computer Science, University of Indonesia
DKI Jakarta, 10430, Indonesia
dian.ismiati@ui.ac.id
dian.ismiati@gmail.com

Panca Oktavia Hadi Putra
Faculty of Computer Science, University of Indonesia
DKI Jakarta, 10430, Indonesia
hadiputra@cs.ui.ac.id

Abstract

Indonesia's banking industry is evolving in personal data management due to technological advancements, presenting opportunities and challenges. Influenced by global standards like the General Data Protection Regulation (GDPR), Indonesia's Law No. 27 of 2022 on Personal Data Protection incorporates similar principles, including the Data Protection Impact Assessment (DPIA) for high-risk data processing, though implementation regulations are pending. This research develops and validates a tailored DPIA framework for the Indonesian banking sector. It offers practical solutions such as risk identification, assessment, and mitigation measures, alongside recommendations for staff training, localized assessment tools, IT integration, and continuous monitoring mechanisms to ensure compliance. By addressing unique challenges like balancing innovation with compliance and safeguarding consumer trust, this study contextualizes global best practices within Indonesia's regulatory framework, providing valuable insights for policymakers, practitioners, and researchers while emphasizing the critical role of DPIAs in enhancing personal data protection and fostering a culture of privacy in the banking sector.

Keywords: Data Protection Impact Assessment, DPIA, Law No. 27/2022, Indonesian Banking, General Data Protection Regulation, Risk Management, Personal Data, IT Application.

Introduction

In a global context, data is often heralded as the new oil, creating a critical importance and a top priority for protecting personal data. Organizations across the globe collect, store, and process vast amounts of personal information, necessitating robust mechanisms to ensure this data is handled responsibly and securely. One such mechanism is the Data Protection Impact Assessment (DPIA), a vital tool designed to help organizations identify and mitigate risks to data privacy and security; this also includes banks that highly value their customer's data.

The banking sector is uniquely positioned as a critical industry that manages susceptible personal and financial information, including account details, transaction histories, credit information, and

* Corresponding Author with contact details, email address, and full postal address

identification documents. This data is fundamental to the functioning of financial systems and the provision of services such as loans, payments, and investments. Mismanagement or breaches of this data can lead to severe consequences, including identity theft, financial fraud, loss of customer trust, and legal or regulatory repercussions. As financial institutions operate in a highly regulated environment, effective data management is crucial to ensure compliance, safeguard consumer rights, and mitigate risks associated with financial crimes. Maintaining strong data protection practices upholds regulatory standards and strengthens public confidence in the banking system.

The banking industry in Indonesia has faced significant transformation in managing its users' personal data. Such transformation is also triggered by the vast development of information and communication technology (ICT) that enables transboundary connections. In this context, ICT has greatly benefited every sector, including e-commerce, e-education, e-health, e-government, and other sectors. The vast technological improvement that has expanded many opportunities also challenges personal data protection.

Following the European Union (EU) enacting the GDPR, in 2022, Indonesia successfully enacted its data protection regulations through the Law No. 27 of 2022 on Personal Data Protection (Law No. 27/2022). This is a significant game-changer for Indonesia to provide robust protection of one's data. In Law No. 27/2022, Indonesia integrates the GDPR principles as its primary reference in personal data protection. One is the Data Protection Impact Assessment (DPIA), further regulated under Article 35 of GDPR.

The assessment process in the DPIA includes four important components: system description evaluation of processing operations in line with the specified objectives, risk assessment to protect the rights and freedoms of data subjects, and anticipated steps to address identified risks (Article 35 GDPR). DPIA functions as a risk mitigation method arising from data processing activities. Under the GDPR, DPIA is essential in personal data protection regulations. It enables organizations, including the banking sector, to identify potential risks associated with personal data processing. In this way, DPIA plays a crucial role in maintaining individual privacy and managing risks that may threaten public trust and regulatory compliance.

In Indonesia, the regulations explicitly addressing DPIA in the banking sector are also outlined in POJK No. 11/POJK.03/2022, which mandates that banks must implement personal data protection principles when processing personal data. Should conditions arise that potentially increase risks to personal data owners, banks must conduct an impact assessment regarding applying personal data protection principles as stipulated.

Based on the author's research, previous studies have not explicitly focused on the banking sector. For instance, research by López et al. (2021) focused on identity management technology, while Yungratog et al. (2022) discussed data protection risks in the maritime industry. Therefore, this study is among the first to develop and test a DPIA framework specifically tailored for the banking sector in Indonesia.

The regulations in Indonesia, specifically in the Indonesian banking sector regarding DPIA, or in Indonesian known as *Penilaian Dampak Perlindungan Data Pribadi*, are found in the statutory provisions and applicable regulatory provisions, including, among others, Law No. 27 of 2022 concerning Personal Data Protection and POJK No. 11 of 2022 concerning the Implementation of Information Technology by Commercial Banks.

In Law No. 27/2022, the regulation of DPIA is stipulated under Article 34, which mandates that Personal Data Controllers must conduct a DPIA when the processing of Personal Data carries a high potential risk to Personal Data Subjects. The law further explains that further provisions regarding the impact assessment of Personal Data Protection will be regulated in Government Regulations. As of today, the said Government Regulation has yet to be enacted. However, the said bill of the Government Regulation has been provided for a public review. The bill has outlined several minimum requirements that must be included in the DPIA.

This paper will discuss the development of a DPIA framework in the Indonesian banking sector under Law No. 27/2022. The objective is to uncover best practices in conducting DPIA as a framework for managing and protecting customer personal data. This paper will analyze the component of Law No.

27/2022 in the banking sector and combine the current best practices experience and assessment tools for GDPR with a specifically developed framework to measure the preparedness and readiness of Indonesian banking in compliance with Law No. 27/2022. This will help banking sectors understand the requirements under Law No. 27/2022, identify which area needs to be improved and enhance their compliance with Law No. 27/2022. The systematic literature review (SLR) is based on the following questions:

1. What components constitute the framework for DPIA in Indonesian Banking under the UU PDP?
2. How can the framework instruments measure Data Protection Impact Assessment in Indonesian Banking under the UU PDP?
3. How can these instruments be validated through case studies in Indonesian banking?

Literature Review

DPIA: Views From the European Union and Indonesia

DPIA in the European Union

DPIA, under Article 35 of the GDPR, is a process that systematically examines how personal data is processed and evaluates the potential risks that such processing may pose to the privacy and security of individuals (General Data Protection Regulation, n.d.). This assessment is not just a regulatory checkbox but a proactive approach to data protection, emphasizing the need for privacy by design and default. By conducting a DPIA, organizations can foresee potential privacy issues before they become problematic, allowing them to implement measures that protect personal data effectively. Under Article 35 of the GDPR, a DPIA must include a detailed description of the intended processing activities and their purposes, an evaluation of the necessity and proportionality of these activities about their goals, an assessment of the potential risks to individuals' rights and freedoms, and the measures planned to mitigate these risks. These measures should ensure personal data protection, demonstrate compliance with the GDPR, and consider the rights and legitimate interests of the affected individuals and other stakeholders.

The concept of DPIA has been significantly highlighted by the General Data Protection Regulation (GDPR) that took effect in May 2018. Under the GDPR, DPIAs are mandatory for processing activities that are likely to result in a high risk to the rights and freedoms of individuals. This includes large-scale processing of sensitive data, systematic monitoring of public areas, and any other operations that could potentially have significant privacy implications. By requiring DPIAs, the GDPR aims to ensure that data protection is an integral part of the data processing lifecycle rather than an afterthought. The DPIA is required if the controller uses the latest technologies in consideration of the nature, scope, contexts, and objectives of the processing, which may create a high risk to one's freedom and rights.

DPIA Guidelines Under the Article 29 Data Protection Working Party

Before the establishment of the European Data Protection Board and the enactment of the GDPR, the Article 29 Working Party (the A29WP), which dealt with issues relating to the protection of privacy and personal data, issued data protection directives (The European Data Protection Board, 2018).

The A29WP created a guideline on the DPIA and determined whether the data processing is considered "likely to result in high risk" by the GDPR 2016/679 in the EU. The basic principle of DPIA in GDPR is shown in the following scheme as shown in Figure 1.

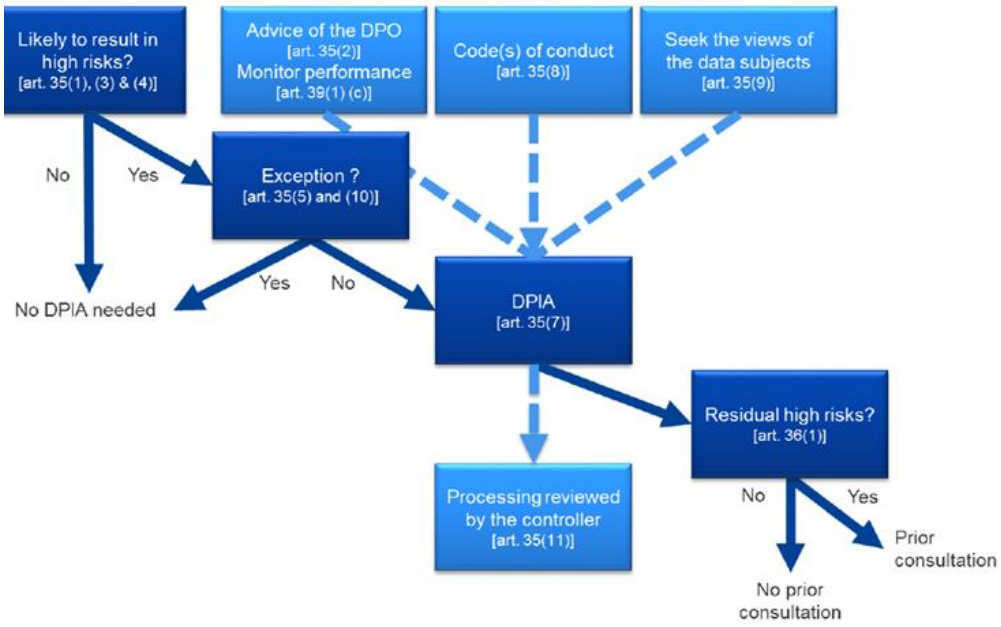

Figure 1. Fundamental DPIA Principle under the GDPR

DPIA on Law No. 27/2022 on Personal Data Protection and Bill of Government Regulation on Personal Data Protection

Law No. 27/2022 obligated the data controller to assess the impact of Personal Data Protection (or, in short, the DPIA) if processing such personal data has a high-risk potential to the Personal Data subject. Law No. 27/2022 provides a threshold for processing personal data that is considered high-risk and further mandates that any technical implementations regarding personal data processing shall be regulated under specific Government Regulations. However, to this date, the Indonesian Government is still carefully deliberated the bill.

Even though the bill has yet to be enacted, the bill is available for the public to see the latest updates (Bill of Indonesian Government Regulation on Personal Data Protection, 2024). The bill has included the proposed obligations to conduct DPIA before processing high-risk personal data. The DPIA further must consist of the following:

1. A systematic description of the Personal Data processing activities and the purposes of Personal Data processing, including the interests of the Personal Data Controller in this processing;
2. An assessment of the necessity and proportionality between the purposes and the Personal Data processing activities;
3. An assessment of the risks to the protection of the rights of Personal Data Subjects and
4. Measures the Personal Data Controller uses to protect Personal Data Subjects from the risks of Personal Data processing.

Regulation of the Financial Services Authority (Otoritas Jasa Keuangan) of the Republic of Indonesia No. 11/POJK.03/2022 on the Organization of Information Technology by Commercial Banks

Regarding data protection, banks are obligated to manage data effectively to support the achievement of business objectives of such banks (OJK Regulation No. 11/POJK.03, 2022). Further, under OJK Regulation No. 11/POJK 03 (2022), banks must implement personal data protection principles in processing personal data. They shall also conduct an impact assessment upon implementing personal data protection principles in which, in certain conditions, such data can potentially increase the risks of personal data owners.

The OJK Regulation No. 11/2022 commentary states that personal data protection principles must comply with the current laws and regulations on personal data protection. Additionally, the commentary on Article 44 paragraph (2) outlines specific conditions that must be met, which include actions such as the use of new technologies, tracking customers' locations and behaviors, large-scale monitoring of public facilities, and processing sensitive personal data related to ethnicity, religion, race, and intergroup relations.

Methodology

Research Database Search and Keywords

The research targets international studies on frameworks or readiness assessment instruments related to technology and information systems. Databases used include Google Scholar, Science Direct, ACM Digital Library, and Elsevier (Scopus), with keywords: ("assessment" OR "tools" OR "framework") AND (“Data Protection Impact Assessment” OR “DPIA”) AND (“Banking” OR “Financial”).

Criteria for selecting research include:
1. Publications from the last five years (2019-2023).
2. Publications in journals or proceedings.
3. Full-text publications.
4. Publications in English.

3,564 documents were obtained: 144 from ScienceDirect, 62 from Elsevier Scopus, 3,320 from Google Scholar, and 38 from ACM Digital Library. The documents were then screened according to the above criteria, resulting in six documents relevant to the research questions, which can be seen in López et al. (2021), Demetzou et al. (2019), Horák et al. (2019), Chatzipoulidis et al. (2019), Dashti and Ranise (2020) and Yungratog et al. (2022).

We conducted a Literature Review using the PRISMA methodology. PRISMA is a widely used health and social sciences method for conducting literature reviews. This method is an organized and transparent approach with guidelines for performing and reporting systematic reviews. The process involves several stages, such as identifying and selecting relevant studies, extracting and analyzing data, synthesizing findings, assessing the quality of evidence, and presenting results as shown in Figure 2.

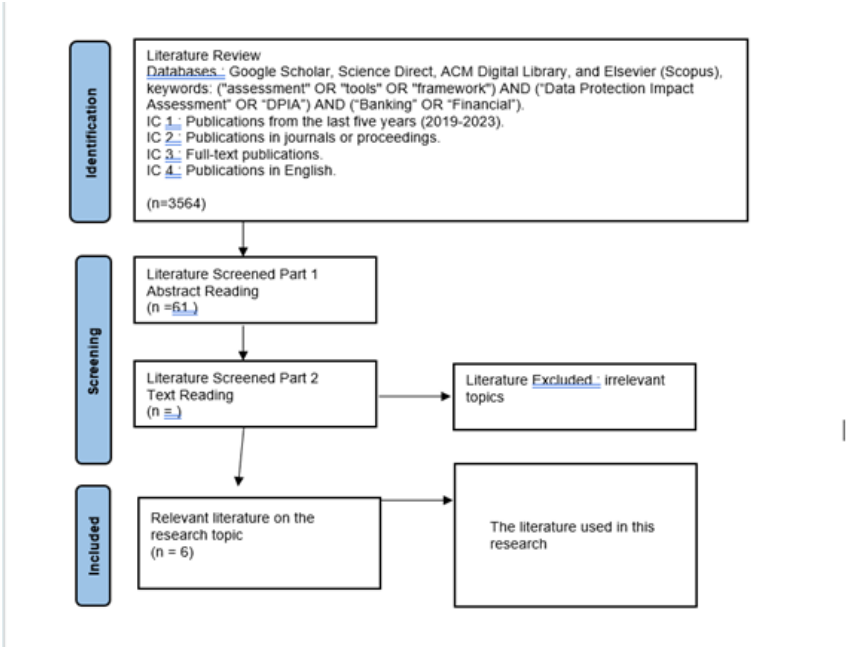

Figure 2. PRISMA SLR (Modified)

The results from the obtained documents, along with a case study referring to primary and secondary sources (e.g., writing references, documents, observation, and interviews), are utilized to analyze the

issues arising from the DPIA under Law No. 27/2022 to address the research questions. After obtaining the abovementioned instruments, the 3 (three) independent raters will be measured using Inter-Rater Reliability with Fleiss' Kappa. Inter-rater reliability (IRR) is a crucial component in qualitative research to ensure consistent interpretation of data among multiple raters. Fleiss' Kappa is one of the statistics used to measure IRR, especially when there are more than two raters.

Fleiss' Kappa is a statistical measure used to evaluate the level of agreement between multiple raters when assigning categorical ratings to a set of items. Unlike Cohen's Kappa, which is suitable for two raters, in the context of validating the framework instrument developed for the Personal Data Protection Impact Assessment (DPIA) in the banking sector in Indonesia, the Fleiss Kappa method was implemented to measure the level of agreement between raters. Fleiss 'Kappa accommodates assessments by more than two raters, making it an appropriate choice for this study, where three experts evaluated the proposed framework.

Fleiss' Kappa ensures the instrument's reliability by quantitatively measuring the consistency of ratings among the legal expert, the Data Protection Officer (DPO) from Bank XYZ, and the academic researcher. This method highlights areas of agreement and disagreement, providing insights into the clarity and robustness of the framework.

Fleiss' Kappa is particularly suited for studies that involve subjective assessments and qualitative judgments, as it accounts for the possibility of agreement occurring by chance. Its application in this research aligns to ensure a robust and validated framework for conducting DPIAs in the Indonesian banking sector.

The following are the steps for calculating Fleiss' Kappa that will be carried out by the author based on the method described in Cole (2023):

1. Determining the Experts as the Independent Raters

   The Independent Raters chosen are the DPO of Bank XYZ, the Legal of Bank XYZ, and Academics.

2. Data Preparation

   Collection of evaluation by the Independent Raters which is a table consisting of the Independent Experts' rates with the categories of "Suitable" and "Not Suitable".

3. Calculating Frequencies

   Further will calculate the total rates of every question given to the Independent Raters.

4. Calculating Proportions

   After calculating the frequency, the next step is to calculate the proportion. Proportion describes the share of raters who chose each answer category for each question to obtain a more detailed picture of the distribution of answers among raters.

   In calculating the proportion, the first step is to calculate the actual proportion of agreement ($\bar{P}$), namely the average agreement between raters for each question *i*, the proportion of agreement *Pi*.

$$Pi = \frac{1}{n(n-1)} \sum_{k=1}^{k} nik\ (nik - 1)$$

   Information:

   - *n* is the number of raters
   - *k* is the number of answer categories
   - *nik* is the number of raters who chose answer category k for question i.

   After calculating *Pi* for all questions, further is to calculate the average ($\bar{P}$)

$$\bar{P} = \frac{1}{N}\sum_{i=1}^{N} Pi$$

Information:

- *N* is the number of questions

Then, calculate the expected proportion of agreement by chance ($\overline{(Pc)}$), namely the average of the expected proportion of answers based on the frequency of answer categories in all questions.

The proportion for each answer category is calculated by dividing the number of assessors who chose that category by the total number of assessments using the following formula:

$$Pj = \frac{1}{Nn}\sum_{i=1}^{N} nij$$

Information:

- *Pj* is the proportion of answer *j*
- *N* is the number of questions
- *n* is the number of questions
- *nij* is the number of raters who chose category j for question i.

Then calculate ($\overline{(Pc)}$) by adding the squares of all Pj as follows:

$$\overline{Pc} = \sum_{j=1}^{k} Pj^2$$

By calculating frequencies and proportions, researchers can understand how answers are distributed among raters and prepare data for the next step in calculating Fleiss' Kappa.

5. Calculating Kappa Value

After obtaining the actual agreement proportion and the proportion expected by chance, the next step is to calculate the Kappa value using the following formula:

$$k = \frac{\bar{P} - \overline{Pc}}{1 - \overline{Pc}}$$

Information:

- $\bar{P}$ is the proportion of actual deals
- $\overline{Pc}$ is the proportion expected by chance?

6. Interpretation of Results:

The last step is to interpret the Fleiss' Kappa values to determine the level of inter-rater agreement:

- 0.01–0.20: Slight agreement
- 0.21–0.40: Fair agreement
- 0.41–0.60: Moderate agreement
- 0.61–0.80: Substantial agreement
- 0.81–1.00: Almost perfect agreement.

Discussion

Connections between A29WP and the European Data Protection Board

As previously mentioned, before the establishment of the European Data Protection Board (EPDB), the independent *advisory body* function done by the A29WP which was established under the directives of Article 29 Directive 95/46/EC back in 1995. With the GDPR fully enacted, the A29WP became the EPDB as of 25 May 2018. Even though the advisory body has changed, all the prior guidelines, recommendations, and documents produced under the A29WP are still in force and have been endorsed by the EPDB through its first plenary on 25 May 2018. Currently, the DPIA Guidelines are still in force and the legit reference for the enforcement guidelines for DPIA practices by data controllers under the GDPR.

Current Status of Government of Indonesia's Regulation Bill on Personal Data Protection

Article 34 paragraph (3) Law No. 27/2022 mandated the Government to create an implementing regulation on the practice of the DPIA and other aspects of Personal Data Protection. However, up to this date, the current bill is still undergoing internal consultation within the ministries; the public does have access to the bill based on the draft as of September 2023. The draft has identified and inserted the criteria for conducting DPIA, such as the GDPR's DPIA requirements and guidelines.

Comparison between Indonesia and EU's Practices on DPIA

After carefully analyzing and comparing both regulations between Indonesia's Law No. 27/2022 and its bill of Government Regulation with the GDPR and DPIA Guidelines, Table 1 describes the main framework of both regulations.

Table 1. Comparisons between Indonesia and the EU on DPIA

Indonesia **(Law No. 27/2022 and Bill of Govt Reg)**	**European Union** **(GDPR and A29WP)**
Provide a systematical description of personal data processing	A systematic description of the processing is provided (Art. 35(7)(a)): ▪ Nature, scope, context, and purpose of the processing are taken into account (recital 90); ▪ Personal data recipients and period for which the personal data will be stored and recorded; ▪ A functional description of the processing operation is provided; ▪ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified; ▪ compliance with approved codes of conduct is taken into account (Article 35(8) ;
Assessment of necessity and proportionality of the objectives and activity of personal data processing	Necessity and proportionality are assessed (Article 35(7)(b)):

Indonesia **(Law No. 27/2022 and Bill of Govt Reg)**	**European Union** **(GDPR and A29WP)**
	▪ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account: o measures contributing to the proportionality and the necessity of the processing based on: • specified, explicit and legitimate purpose(s) (Article 5(1)(b)); • lawfulness of processing (Article 6); • adequate, relevant, and limited to what is necessary data (Article 5(1)(c)); • limited storage duration (Article 5(1)(e)); o measures contributing to the rights of the data subjects: • information provided to the data subject (Articles 12, 13 and 14); • right of access and to data portability (Articles 15 and 20); • right to rectification and to erasure (Articles 16, 17 and 19); • right to object and to restriction of processing (Articles 18, 19, and 21); • relationships with processors (Article 28); • safeguards surrounding international transfer(s) (Chapter V); • prior consultation (Article 36).
Inclusion of risk assessment for protecting the rights of Personal Data Subject	Risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)): ▪ origin, nature, particularity, and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:

Indonesia (Law No. 27/2022 and Bill of Govt Reg)	European Union (GDPR and A29WP)
	○ Risk sources are taken into account (recital 90); ○ potential impacts on the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification, and disappearance of data; ○ threats that could lead to illegitimate access, undesired modification, and disappearance of data are identified; ○ likelihood and severity are estimated (recital 90); ▪ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
Measures used by the Personal Data Controller to protect Personal Data Subject from the risks of personal data processing activity	Interested parties are involved: ▪ The advice of the DPO is sought (Article 35(2)); ▪ The views of data subjects or their representatives are sought where appropriate (Article 35(9)).

Components in the DPIA Framework for Banks in Indonesia on the Implementation of Law No. 27/2022

To address the first research question, the author developed the framework components based on the discussions presented in Chapter 2 and the points outlined in sections 1 and 2 above. This development refers to POJK No. 11/POJK.03/2022, which mandates that in circumstances with the potential to increase risks for personal data owners (as per this regulation, referring to bank customers and/or prospective customers), banks must conduct an impact assessment on the implementation of personal data protection principles. These principles and personal data definitions align with the provisions of personal data protection regulations. Such conditions include using new technologies, tracking customer locations and behavior, monitoring large-scale public facility locations, and processing sensitive personal data about ethnicity, religion, race, and intergroup affiliation.

The methodology used to analyze the components of the Personal Data Protection Impact Assessment (DPIA) framework consists of three steps based on the approach outlined by Dashti et al. (2019): Processing Analysis, Risk Analysis, and Execution Time Analysis. This three-step grouping is not only informed by Dashti et al. (2019) but also by the guidelines in the *"Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for Regulation 2016/679."* These guidelines emphasize a structured approach to ensure comprehensive risk assessment and mitigation.

1. The first step, Processing Analysis, aligns with Article 35(7)(a) of the GDPR.
2. The second step, Risk Analysis, corresponds to Articles 35(7)(c) and (d) of the GDPR.
3. The third step, Real-Time Execution Analysis, involves continuous monitoring and review, as Article 35(11) of the GDPR mandates.

These steps were adopted and adjusted to the Indonesian Personal Data Protection Law (UU PDP) provisions and its Draft Government Regulation (RPP PDP) to ensure a comprehensive and iterative approach to PDPDP. This approach integrates legal and technical aspects of data protection as required by the UU PDP, ensuring the effective identification and management of relevant risks and providing a robust framework for protecting the rights and freedoms of data subjects. Figure 3 shown the proposed framework.

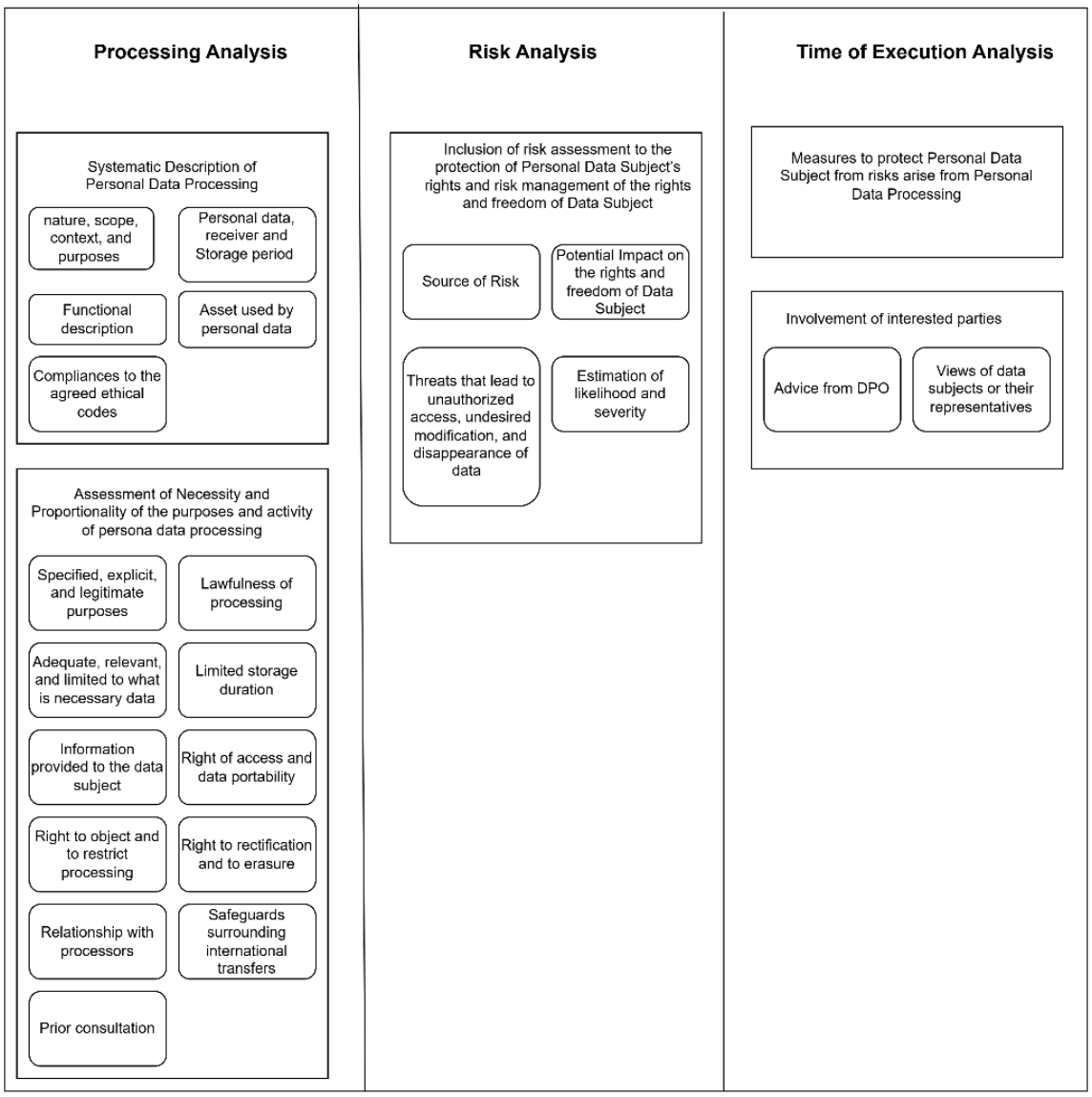

Figure 3. Proposed Framework of DPIA in Indonesia

Instruments derived from the Framework of DPIA and the Applicability to measure DPIA in Indonesian Banks

After determining the above-mentioned framework, the next step is to create an instrument by applying a layered DPIA methodology. The first layer ensures whether the processed data is categorized as personal data or risk analysis (multiplication of probability times impact). The second layer consists of a review of compliance levels with data protection principles within the specific scope of data processing.

After the abovementioned analysis, the following are the combined instruments from Law No. 27/2022 and Bill of Government Regulation on Personal Data Protection with the GDPR and A29WP, which can be seen in Table 2.

Table 2. Instruments to Measure DPIA in Indonesian Banks

Scope	Instrument	Measuring Questions
First Layer: **Fulfillment of criteria of processed data that can be categorized as personal data, risk analysis (multiplication of probability times impact)**	Initial Assessment: In this initial assessment process, the Personal Data Controller must conduct an assessment on DPIA if the said processing has a potential of being high risk to the Personal Data Subject, in line with the criteria mentioned under Law No. 27/2022.	Is DPIA necessary to be done in line with Law No. 27/2022 and the Bill of Government Regulation on Personal Data Protection?
	1. Automatic decision-making that can cause legal consequences or significant impact on the Personal Data Subject.	1. Does Personal Data Processing involve automated decision-making that could have legal consequences or significantly impact the Personal Data Subject?
	2. Personal Data Processing with specific personal data.	2. Does the Personal Data Processing use specific personal data?
	3. Large-scale Personal Data Processing.	3. Is the Personal Data Processing carried out on a large scale?
	4. Processing of personal data that includes systematic evaluation, scoring, or monitoring activities of Personal Data Subject.	4. Does the processing of personal data include systematic evaluation, scoring, or monitoring activities of the Personal Data Subject?
	5. Data Processing includes activities of matching or combining groups of personal data.	5. Does processing personal data involve matching or combining groups of personal data?
	6. Usage of the latest technology in personal data processing	6. Does the processing of personal data use the latest technologies?
	7. Processing of personal data limits the exercise of the Personal Data Subject's rights.	7. Does the processing of personal data limit the exercise of Personal Data Subjects' rights?

Scope	Instrument	Measuring Questions
Personal Data Processing Activity	Systematic Description of the processing and the purposes of the processing, including the interest of the Personal Data Controller.	8. What purpose will be achieved by processing the Personal Data? 9. Has the lawful processing basis for processing such activities been determined?
	Calculation of nature, scope, context, and purpose of processing	10. Who is the Data Subject in Personal Data Processing? 11. What kind of Personal Data is used in Personal Data Processing?
	Recording of personal data, recipients, and storage period of personal data	12. Has there been a scheduled deletion for data and/or information that has exceeded the Personal Data storage period?
	Provision of functional description of processing operations.	13. Are the functional descriptions and processing operations available?
	Identification of assets that personal data is used on (hardware, software, networks, people paper, or similar transmission channels).	14. What assets will use the personal data?
	Compliance with the agreed ethical code	15. Is the Personal Data Processing for the stated and specified purposes not in conflict with the prevailing laws, code of conduct, or any public policy?
Purpose and Activity of Personal Data Processing	Assessment of the need and proportionality between the purposes and activities of Personal Data Processing	16. Is the Personal Data Processing carried out according to the purpose and needs conveyed to the Personal Data Subject, and are there no other needs?
	Specified, explicit, and legitimate purposes	17. Is the collection of Personal Data carried out for stated, specified, explicit, and legitimate purposes? 18. Is the Personal Data Processing carried out by the consent of the Personal Data Subject?
	Lawfulness of processing	19. Is there a process to ensure that the Personal Data used remains accurate and complete?

Scope	Instrument	Measuring Questions
	Adequate, relevant, and limited to what is necessary data	20. Is there a process to ensure that the Personal Data used is adequate, accurate, and limited to what is necessary?
	Limited storage duration	21. Will the processing of Personal Data follow the Personal Data retention schedule that applicable internal rules or regulations have determined? 22. Describe the appropriate steps to destroy or de-identify Personal Data if it is no longer needed.
	Information provided to the data subject	23. In Personal Data Processing activity, does the Data Subject request information regarding clarity of identity, the basis for legal interest, the purpose of requesting and using Personal Data, and the responsibilities of the party requesting Personal Data?
	Right to access and to data portability.	24. In Personal Data Processing, can the Data Subject obtain access and a copy of his/her Personal Data by the prevailing laws and regulations?
	Right to rectification and to erasure	25. In Personal Data Processing, whether the Data Subject makes corrections (completing, updating, and/or correcting errors and/or inaccuracies in their own Personal Data) and/or deletes/destroys Personal Data provided to the Personal Data Controller?
	Right to object and to restrict processing.	26. In Personal Data Processing, whether the Data Subject can object to or limit the processing of Personal Data?
	Relationships with processors	27. Does the Personal Data Subject know the identity of the data controller or the organization or entity that processes their Data?
	Safeguards surrounding international transfers	28. Whether the processing of Personal Data only include sending data within the domestic area or include transboundary?
	Prior Consultation	
Risk Assessment	Risk Assessment of the protection of Personal Data Subject's rights	29. Are Personal Data Subjects aware of the risks that may occur and the security measures taken in processing their Data?

Scope	Instrument	Measuring Questions
	Risk management of the rights and freedom of Data Subject	30. How do we manage risks to the rights and freedom of Data Subjects?
	Tally of Source of Risks	31. Are there any security issues previously occurring in processing Personal Data?
	Identification of threats that could lead to illegitimate access, undesired modification, and disappearance of data	32. Is Personal Data processed on this system encrypted in transit or stored?
	Identification of threats that could lead to illegitimate access, undesired modification, and disappearance of data	33. Is there any identification of risks that lead to illegitimate access, undesired modification, and disappearance of data?
	Estimation of severity	34. Is there any review of the incident to be used as a learning material and update the related system/program?
Protection of the Personal Data Subject from Risks	Measures to be taken by the Personal Data Controller to protect Personal Data Subject from risks of personal data processing	35. Have the data security principles been implemented in Personal Data Processing? 36. Is there any regular training for staff regarding data security?
	Determining anticipated measures to handle risks	37. Have any anticipatory steps been determined to handle risks?
	Involvement of interested parties, such as: ○ Advice from Data Protection Officer ○ Views of Data subjects or their representatives, where appropriate.	38. Are the Personal Data Subjects provided with information on how to contact the Data Protection Officer (DPO)? 39. Does Personal Data Processing involve the Data Protection Officer (DPO)?

Instruments Validation Through Case Study in The Banking Sector in Indonesia

The abovementioned instruments are validated through the Fleiss Kappa method, which is depicted in Table 3.

Table 3. Results of Validation of Instrument Using Fleiss' Kappa Method

Question(s)	Rater 1	Rater 2	Rater 3	Total Suitable	Total Not Suitable	*Pi*
1	Suitable	Suitable	Suitable	3	0	1
2	Suitable	Suitable	Suitable	3	0	1
3	Suitable	Suitable	Suitable	3	0	1
4	Suitable	Suitable	Suitable	3	0	1
5	Suitable	Suitable	Suitable	3	0	1
6	Suitable	Suitable	Suitable	3	0	1
7	Suitable	Suitable	Suitable	3	0	1
8	Suitable	Suitable	Suitable	3	0	1
9	Suitable	Suitable	Suitable	3	0	1
10	Suitable	Suitable	Suitable	3	0	1
11	Suitable	Suitable	Suitable	3	0	1
12	Suitable	Suitable	Suitable	3	0	1
13	Suitable	Suitable	Suitable	3	0	1
14	Suitable	Suitable	Suitable	3	0	1
15	Suitable	Suitable	Suitable	3	0	1
16	Suitable	Suitable	Suitable	3	0	1
17	Suitable	Suitable	Suitable	3	0	1
18	Suitable	Suitable	Suitable	3	0	1
19	Suitable	Suitable	Suitable	3	0	1
20	Suitable	Suitable	Suitable	3	0	1
21	Suitable	Suitable	Suitable	3	0	1
22	Suitable	Suitable	Suitable	3	0	1
23	Suitable	Suitable	Suitable	3	0	1
24	Suitable	Suitable	Suitable	3	0	1
25	Suitable	Suitable	Suitable	3	0	1

Question(s)	Rater 1	Rater 2	Rater 3	Total Suitable	Total Not Suitable	*Pi*
26	Suitable	Suitable	Suitable	3	0	1
27	Suitable	Suitable	Suitable	3	0	1
28	Suitable	Suitable	Suitable	3	0	1
29	Suitable	Suitable	Suitable	3	0	1
30	Suitable	Suitable	Suitable	3	0	1
31	Suitable	Suitable	Suitable	3	0	1
32	Suitable	Suitable	Suitable	3	0	1
33	Suitable	Suitable	Suitable	3	0	1
34	Suitable	Suitable	Suitable	3	0	1
35	Suitable	Suitable	Suitable	3	0	1
36	Suitable	Suitable	Suitable	3	0	1
37	Suitable	Suitable	Suitable	3	0	1
38	Suitable	Not Suitable	Not Suitable	1	2	0.33333333
39	Suitable	Suitable	Suitable	3	0	1
				115	2	0.98290598
				0.966104	0.00029221	0.96639638
				fleiss kappa		**0.49130435**

The results show a Fleiss Kappa value of 0.491, which indicates a moderate level of agreement. This indicates that although there is substantial agreement in many aspects, some areas still require improvement in terms of consistency between raters.

Another thing that affects the value of Fleiss Kappa is that the more answers are concentrated in one column, the higher the expected probability, which is undesirable. The more answers are concentrated in the same column for each row, the higher the observed agreement, which is the goal—finally, the greater the difference between the expected and observed probability, the better. In the Validity test carried out in this research, this became an obstacle because the answer choices were only "Suitable" and "Not Suitable," the answers were concentrated in one column; namely, for each rater, there were many.

One of the important findings in this validation process was identifying significant disagreement on the specific question: "*Are Personal Data Subjects provided with information on how to contact the Data Protection Officer (DPO*)?" From these results, two of the three raters expressed disagreement with the instrument.

Factors that influence the rater's perception and assessment include this disagreement originating from variations in the implementation of bank XYZ's policies, where banking institutions in Indonesia have different policies regarding the function and affordability of DPOs, which directly impacts how the raters assess the availability of this information to the subject. Data, in this case, there is a possibility that at Bank XYZ, the DPO is not directly related to the Personal Data Subject, so the measurement question is not appropriate.

Alignment with Previous Research

This study emphasizes the critical role of Data Protection Impact Assessments (DPIAs) in ensuring compliance with data protection regulations, such as the GDPR and Indonesia's Personal Data Protection Law (UU PDP). López et al. (2021) highlight DPIAs' importance in implementing privacy by design within identity management systems, aligning with our findings demonstrating DPIAs' effectiveness in identifying and mitigating risks in Indonesia's banking sector.

Employing a methodology inspired by Dashti et al. (2019), we analyzed DPIA framework components through processing, risk, and execution time analysis, providing a comprehensive evaluation basis. Consistent with prior research, including Yungratog et al. (2022), our study underscores risk analysis as a pivotal DPIA component for managing personal data processing risks within Indonesia's banking industry. These insights contribute to the broader understanding of DPIA implementation, offering practical guidance for enhancing data protection practices in sector-specific contexts.

Divergence from Previous Research

The Indonesian banking sector faces significant shifts in personal data management driven by technological advancements, requiring alignment with global standards like the GDPR. Law No. 27 of 2022 on Personal Data Protection (UU PDP) adopts similar principles, including the mandate for a Data Protection Impact Assessment (DPIA) for high-risk data processing, although specific implementation guidelines remain absent. This study develops and validates a DPIA framework tailored to Indonesia's banking sector. It provides a structured risk assessment and mitigation approach alongside recommendations for localized tools, staff training, process integration, IT automation, and continuous monitoring. This research contextualizes global best practices within Indonesia's legal framework by addressing unique sectoral challenges, such as balancing compliance with innovation and safeguarding consumer trust. It highlights the critical role of DPIAs in fostering a culture of privacy while ensuring regulatory compliance. Additionally, limitations in the validation process, mainly restricted response options, emphasize the need for more nuanced methodologies to enhance accuracy and applicability in future research.

Suggestions

The following suggestions are provided for future researchers:

1. Future researchers are encouraged to use a variety of validation instruments and not rely solely on one method, such as Fleiss' Kappa. Employing multiple validation methods can offer a more comprehensive view and ensure that research results are more accurate and reliable.
2. Future studies should be conducted across various banking institutions in Indonesia, including large and small banks and Islamic banks. This is important to ensure that the findings are generalizable and relevant to the entire banking sector in Indonesia.
3. Future researchers may consider conducting comparative studies between the implementation of DPIA in banking and other sectors, such as healthcare, e-commerce, and telecommunications. Such comparative studies could reveal differences and similarities in implementing DPIA across industries and provide broader insights into best practices for personal data protection.
4. Given the rapid technological advancements, future research should explore the impact of new technologies, such as Artificial Intelligence (AI), on implementing DPIA. These technologies can potentially enhance the accuracy and efficiency of risk assessments and personal data management.

Conclusion

This study successfully develops a comprehensive framework for the Personal Data Protection Impact Assessment (PDPIA), addressing the specific needs of Indonesia's banking sector in alignment with the Personal Data Protection Law (PDP Law). The framework is structured around three core components: processing analysis, which systematically examines the necessity and proportionality of personal data processing activities; risk analysis, which identifies and mitigates risks to the rights and freedoms of data subjects; and execution time analysis, which focuses on implementing protective measures and involving relevant stakeholders during the data processing lifecycle. These components provide a structured approach to understanding and managing data protection obligations.

The proposed methodology integrates these components into a practical, multi-layered system. At the initial stage, the framework ensures the processed data qualifies as personal data and evaluates associated risks based on likelihood and impact. In subsequent phases, compliance with data protection principles is reviewed in the context of the specific processing activities. These instruments are critical tools for enabling Indonesian banks to implement DPIAs effectively and address sector-specific challenges under the PDP Law.

To validate the framework, assessments were conducted by three experts—a legal representative, a Data Protection Officer (DPO) from Bank XYZ, and an academic. Fleiss' Kappa was employed to measure inter-rater agreement, yielding a moderate score of 0.491. While this result confirms the framework's reliability, it also highlights opportunities to enhance the consistency of evaluations. Despite these challenges, the framework offers a practical solution to facilitate compliance with the PDP Law, ensuring the protection of personal data subjects while maintaining operational efficiency.

The study further underscores the importance of integrating IT tools to improve the accuracy and efficiency of the assessment process. It also emphasizes the need for ongoing monitoring and evaluation to sustain compliance and adapt to evolving regulatory requirements. By contextualizing global best practices within Indonesia's regulatory framework, this research provides valuable insights for improving personal data protection in the banking sector. It contributes to the broader discourse on privacy and data governance.

References

Chatzipoulidis, A., Tsiakis, T., & Kargidis, T. (2019). A readiness assessment tool for GDPR compliance certification. *Computer Fraud & Security*, 2019(4), 9-15.

Cole, R. (2023). Inter-Rater Reliability Methods in Qualitative Case Study Research. *Sociological Methods & Research*, 53 (4), 1944-1975.

Dashti, S., & Ranise, S. (2020). Tool-Assisted Risk Analysis for Data Protection Impact Assessment. In Friedewald, M., Önen, M., Lievens, E., Krenn, S., & Fricker, S. (Eds.), *Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019* (pp. 259-276). Springer, Cham.

Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation. *Computer Law & Security Review*, 35.

Horák, M., Václav, S., & Husák, M. (2019). GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform. In *ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security*.

López, C. T., Domingon, I. A., & Torrijos, J. V. (2021). Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals: A special reference to Identity Management Systems. In *ARES 2021: Proceedings of the 16th International Conference on Availability Reliability and Security*, 132, 1-9

The European Data Protection Board. (2018). Legacy: Art. 29 Working Party. https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en

Yungratog, S., Goerlandt, F., Punurai, W., & Thammaboosadee, S. (2022). A Conceptual Framework for Assessing Risks for Data Protection Impact Assessment Process in Maritime Industries. In *2022 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*.

How to cite:

Anggraini, D. I.., & Putra, P. O. H. (2025). Data Protection Impact Assessment Framework in the Banking Sector in Indonesia to Implement Law of Personal Data Protection. *Jurnal Sistem Informasi (Journal of Information System), 21*(1), 15–34.