Eduvest – Journal of Universal Studies
Volume 5 Number 12, December, 2025
p- ISSN 2775-3735- e-ISSN 2775-3727

Regulation of Personal Data Legal Protection in BPJS Ketenagakerjaan Membership, Denpasar Branch Office

Saifullah Hasan*, AAA. Ngurah Sri Rahayu Gorda
Universitas Pendidikan Nasional Denpasar, Indonesia
Email: saifullahhasa@gmail.com*, srigorda@undiknas.ac.id

ABSTRACT

This research analyzes legal protection arrangements for personal data in BPJS Ketenagakerjaan Denpasar Branch membership and examines the institution's responsibilities in safeguarding participants' information. Employing normative juridical methods with statute, comparative, conceptual, and economic law analysis, it draws on secondary legal materials from primary, secondary, and tertiary sources. Findings indicate that personal data protection in BPJS Ketenagakerjaan is governed by Law Number 27 of 2022 on Personal Data Protection and Law Number 24 of 2011 concerning the Social Security Administering Body. As data controller, BPJS Ketenagakerjaan must ensure legitimacy, confidentiality, and security via internal policies, encryption, restricted access, and audits. Yet, the Denpasar Branch faces challenges like limited human resources, low participant awareness, and risks of misuse or cyberattacks. Stronger internal oversight, staff capacity building, and inter-institutional synergy are essential for effective implementation aligned with legal certainty, justice, and human rights. Recommendations include regular security audits, comprehensive data privacy training, clear incident protocols, educational campaigns on data rights, and advanced cybersecurity like multi-factor authentication and real-time monitoring.

KEYWORDS *Personal Data Protection, BPJS Ketenagakerjaan, Legal Responsibility, Data Privacy, Indonesia*

INTRODUCTION

The current era of digitalization transcends limitations of distance, space, and time. Human daily activities in the digital space have become essential to facilitate work. According to a report by Statista (a global business intelligence data platform), as of February 2025, there were 5.56 billion internet users worldwide, representing 67.9% of the world's population. This increase stems from increasingly affordable devices and expands digital infrastructure, enabling people to conduct various activities more easily (Chong et al., 2025; Kaewunruen et al., 2021; Osmundsen & Bygstad, 2022; Prabowo et al., 2023; Wang & Shao, 2024).

Everyone connected to digital devices via the internet carries personal data attached to each user. Personal data, along with digital traces left behind, forms a collection that can be processed into reusable information (Bratina, 2023; Ichhpujani et al., 2019; Muharom et al., 2022; Tømte, 2024). Thus, data has become highly valuable, often called "the new oil." The growing volume and complexity of data also attract cybercriminals, particularly those targeting personal data (privacy infringements). Computerized data theft enables perpetrators to access sensitive information.

Article 28G paragraph (1) of the 1945 Constitution provides the constitutional basis guaranteeing personal data as part of the right to privacy. This provision explicitly mandates everyone's right to protection of personal data, honor, dignity, and security. Privacy is an individual's right not to be disturbed (the right to be let alone). This right also encompasses

control over the use of personal information to prevent misuse that could cause harm. Thus, personal data protection serves as a juridical and administrative mechanism emphasizing responsible management of personal information (Anissa & Multazam, 2024; Antoine et al., 2025; Ketmaneechairat et al., 2024; Saurabh, 2024; Siahaan et al., 2024).

Referring to this conception, the scope of privacy can be classified into four main categories. First, information privacy, which includes regulatory frameworks for acquiring and managing personal data. Second, communication privacy, which protects various media of correspondence and interaction, including telephone conversations and electronic communications. Third, bodily privacy, which safeguards individuals' physical integrity from invasive measures, such as genetic testing and biometric data use. Fourth, territorial privacy, which grants the right to restrict physical access to personal or communal areas or spaces, including regulation of surveillance mechanisms like audio-visual monitoring.

Furthermore, any information related to identification or that could identify a person is defined as the personal data of the data subject. Personal data classification varies, including general and special categories, as stipulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), with reference to the General Data Protection Regulation (GDPR) (Alfitri et al., 2024; Andriana Putri, 2023; Febrian et al., 2025; Rinjani & Firmansyah, 2025).

The PDP Law applies to any individual, public body, or international organization involved in legal proceedings governed by the PDP Law, including personal data processing activities. This applies when such activities occur within the jurisdiction of the Republic of Indonesia. Additionally, the PDP Law covers activities outside Indonesia's jurisdiction that produce legal consequences within it, and/or personal data subjects who are Indonesian citizens abroad. If an entity processes personal data of Indonesian citizens or foreign citizens in Indonesia, compliance with the PDP Law is required. This aims to prevent the rampant misuse of personal data.

According to Check Point Research (CPR) findings, the third quarter of 2024 saw a significant rise in global cyberattacks and personal data breaches. Organizations faced an average of 1,876 attacks per week—a 75% increase from the same period the previous year and 15% from the prior quarter. This underscores the widespread and escalating cyber threats demanding attention from all parties.

In Indonesia, 1.3 billion cyberattack attempts occurred between January and November 2021, mostly targeting e-commerce and financial technology sectors. The May 2021 data breach affecting BPJS Kesehatan participants exposed 279 million records, including Population Identification Numbers (NIK), telephone numbers, and payroll data, causing substantial material losses. This incident highlights the urgency of bolstering data protection infrastructure in public entities. Similarly, the March 2020 Tokopedia hack exposed data from 91 million user accounts and 7 million merchant accounts, later sold on the black market for an estimated US$5,000, sparking discourse on cybercrime victim compensation mechanisms.

In early 2023, alleged data leaks surfaced, including from the Social Security Administration Agency (BPJS) and community data at the Directorate General of Population and Civil Registration (*Dukcapil*) under the Ministry of Home Affairs (*Kemendagri*). Despite the PDP Law's enactment late the previous year, data leaks continued plaguing various institutions.

Major 2023 data leaks in Indonesia included 18.5 million BPJS participant records sold on illegal forums for IDR 153 million. In March, a cyber actor using the pseudonym "Bjorka" posted 19.5 million records titled *BPJS Ketenagakerjaan* Indonesia 19 Million on BreachForums, sharing 100,000 samples with Population Identification Number (NIK), full names, dates of birth, addresses, mobile numbers, email addresses, job types, and company names. In May 2023, Bank Syariah Indonesia (BSI) suffered a breach involving 1.5 terabytes of data, including 15 million user records, internal passwords, and customer loan information. These incidents reveal significant gaps in data risk governance—both technical and policy-related—necessitating stronger preventive measures.

Although Indonesia has enacted the PDP Law, administrative sanctions and extrajudicial resolutions predominate, while government regulations as technical rules remain in draft form, limiting enforcement. Given cross-border cyber threats and rising cybercrime, harmonizing the legal framework for personal data protection is essential, including independent periodic monitoring and strict criminal sanctions for deterrence.

The PDP Law was enacted as *lex specialis* to safeguard individuals' rights to their personal data amid rapid digital transformation and rampant leaks in public and private sectors. It addresses public concerns over unauthorized data use. In its considerations, the PDP Law recognizes personal data as a constitutionally protected fundamental right and mandates a dedicated supervisory institution for enforcing norms and sanctions in criminal and administrative domains.

A core norm in the PDP Law is the principle of consent, requiring data controllers to obtain explicit approval from data subjects before processing, with withdrawal rights. This is supported by transparency—controllers must clearly communicate processing policies and purposes—and accountability, mandating internal audits, documentation, and incident reporting to authorities.

Implementing these principles should empower consumers in the digital ecosystem and build trust by minimizing misuse risks. Their effectiveness hinges on complete implementing regulations detailing consent formats, leak reporting, and audit procedures. Thus, a credible supervisory institution is vital for objective oversight of public and private actors, plus appropriate sanctions.

BPJS Ketenagakerjaan is a public legal entity established under Law Number 24 of 2011 concerning the Social Security Administration Agency (BPJS Law), tasked with administering the Employment Social Security program. This includes Work Accident Insurance (JKK), Death Insurance (JKM), Old Age Insurance (JHT), Pension Insurance (JP), and Job Loss Insurance (JKP). To deliver these, *BPJS Ketenagakerjaan* processes personal data in membership management.

Per BPJS Law Article 1 paragraph (4), participants include everyone, including foreigners working at least six months in Indonesia, who pay contributions. Article 10 outlines duties such as: (a) conducting/receiving participant registration; (b) collecting contributions from participants and employers; (c) receiving government contribution aid; (d) administering social security funds for participants; (e) collecting and managing program participant data; (f) paying benefits or financing health services per program rules; and (g) providing program information to participants and the public. Thus, Article 10 mandates collecting and managing participant data.

Article 15 paragraph (2) requires employers, when registering, to provide complete and accurate data on themselves, workers, and families to BPJS. This imposes a legal obligation on participants to submit personal data, serving public interests in state administration, particularly social security. The PDP Law's explanatory notes for Article 15 letter (c) define "public interest in state administration" as including population administration, social security, taxation, customs, and electronic business licensing.

BPJS Ketenagakerjaan's June 2024 membership report recorded 58.80 million participants—65.99% active and 34.01% inactive—a 4.68% rise from June 2023. This reflects a growing volume of data requiring management, with an upward yearly trend.

The *BPJS Ketenagakerjaan* Denpasar Branch, managing Denpasar City labor participation, also shows rising participant data annually. Per the Q1 2025 employment social security report for Denpasar, March 2025 participants totaled 224,128 workers—a 7.74% increase from 208,036 in September 2024. This growth heightens personal data processing demands, necessitating robust legal protections for *BPJS Ketenagakerjaan* participants.

This research's novelty lies in its comprehensive analysis of personal data protection at *BPJS Ketenagakerjaan* through constitutional, administrative, and economic law lenses. Unlike prior studies on general or other-sector data protection, it targets *BPJS Ketenagakerjaan*'s unique challenges as a mandatory institution handling millions of workers' sensitive data. It also empirically examines Denpasar Branch operations, revealing implementation gaps unaddressed in existing literature.

Based on the presented background, this study examines Regulation of Personal Data Legal Protection in *BPJS Ketenagakerjaan* Membership, Denpasar Branch Office and *BPJS Ketenagakerjaan*'s legal responsibilities in safeguarding participant data. The general objective is to analyze legal protections for personal data in *BPJS Ketenagakerjaan* participation. Specific objectives include reviewing regulations on participant data protection and *BPJS Ketenagakerjaan* Denpasar Branch's responsibilities in ensuring data confidentiality and security. Theoretically, it advances legal science on personal data regulation at *BPJS Ketenagakerjaan* and enriches related literature. Applicatively, it informs students, communities, academics, and policymakers on implementation, supporting more comprehensive Indonesian data protection regulations.

METHOD

Legal materials were limited to secondary sources: primary materials such as the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 40 of 2004 concerning the National Social Security System, Law Number 24 of 2011 concerning the Social Security Administering Agency, and Law Number 6 of 2023 concerning the Determination of Government Regulation in Lieu of Law Number 2 of 2022 concerning Job Creation into Law; secondary materials including books and journals; and tertiary materials such as official websites.

Legal materials were collected through literature studies, reviewing relevant documents, records, and reports. These were then classified, analyzed, and interpreted to propose solutions. Analysis was qualitative, descriptive, and analytical, employing statute, comparative, economic analysis of law, and conceptual approaches. The economic law perspective evaluated personal data protection as a legal obligation and economic asset impacting *BPJS*

Ketenagakerjaan's sustainability, including cost-benefit implications of measures, data's economic value, breach liabilities, and the balance between compliance costs and service efficiency.

RESULT AND DISCUSSION

Legal Protection of Personal Data in BPJS Employment Membership Denpasar Branch Office

BPJS Ketenagakerjaan, as a public legal institution established through Law Number 24 of 2011, has the responsibility to organize an employment social security program for all workers. In its implementation, this institution collects personal data belonging to participants, including identities such as names, Population Identification Number (NIK), domicile address, income details, and employment history. Because it includes sensitive information, it must obtain legal protection to avoid potential abuse and violation of the individual's right to privacy.

In Indonesia, the right to privacy has been protected in the constitution since the 2000 amendment, which added 10 human rights items.7 Articles 28 G and 28H of the 1945 Constitution expressly regulate the right to privacy. In addition, there are also some other laws and regulations. Therefore, since the Second Amendment in 2000, the right to privacy is expressly stated in the Constitution of the Republic of Indonesia, namely the 1945 Constitution. Article 28G (1) of the 1945 Constitution contains provisions that recognize the human right to privacy and inviolable freedom, which reads "Everyone has the right to the protection of his or her personal life, family, honor, dignity, and property under his or her control, as well as the right to a sense of security and protection from the threat of fear.

In addition to laws and regulations, ministerial regulations stipulate and regulate the right to privacy. As per the guidelines set by the Ministry of Communication and Information, personal data refers to certain personal information that is stored safely, safely, and authentically secured and treated confidentially. Paragraph (3) of Article 17 of the Regulation of the Minister of Communication and Information Technology No. 12 of 2016 states that telecommunication companies are obliged to maintain the privacy of user information and/or identity. The regulation stipulates that internal personal data protection regulations that consider the use of technology and human resources must exist and be approved for use with electronic devices that can be used in the stage of securing personal data. The right to data confidentiality and the ability to lodge complaints is owned by the owner of the personal data, to resolve disputes regarding his personal data, the right to access past personal data, and the right to request the destruction of certain personal data.

Especially in the Denpasar Branch Office area, the collection of participants' personal data is carried out through online and offline registration mechanisms coordinated by BPJS and HRD officers of the company. The collected data will be processed for the purposes of membership verification, contribution calculation, and the claim process for guarantee programs such as Old Age Insurance (JHT), Work Accident Insurance (JKK), and Death Insurance (JKM). Therefore, the regulation and protection of participants' personal data is a fundamental aspect to ensure public trust in the implementation of social security.

Within the framework of national law, regulations related to the management of personal data of *BPJS Ketenagakerjaan* participants generally refer to the provisions of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law regulates the

basic principles of data protection such as legality, transparency, purpose limitation, accuracy, integrity and confidentiality, as well as the responsibility of data controllers. *BPJS Ketenagakerjaan* as a data controller is obliged to ensure that the entire data collection and processing process is carried out lawfully, limited to public service purposes, and protected from illegal access or processing.

At the implementation level, *BPJS Ketenagakerjaan* Denpasar Branch Office has developed a web-based and mobile application system to facilitate services. However, the use of this electronic system brings new challenges in the form of the threat of data leakage, misuse of access by internal individuals, and the potential for system hacking. Therefore, adequate technical arrangements are needed to implement the principle of security as stipulated in Article 39 of the PDP Law, namely the obligation to take appropriate technical and organizational steps in protecting personal data from the risk of loss, unauthorized access, disclosure, and illegal modification.

As part of its legal responsibilities, the Denpasar Branch Office has also adopted internal data protection policies, including user authentication systems, information encryption, and position-based access restrictions. However, a study by Lestari and Sudarma (2023) noted that there is still a gap between formal regulations and technical implementation in the field, where not all officers fully understand the legal principles of personal data and there is no special complaint mechanism in the event of data misuse1.

In addition to the technical aspect, the aspect of participant rights is also important to pay attention to. Under the PDP Law, participants have the right to know the personal data collected, the right to correct the information, revoke consent to data processing, and request deletion of data if it is no longer relevant. These rights should be guaranteed by BPJS, including at branch offices, as part of a commitment to public services based on transparency and accountability.

Legal protection of personal data in the implementation of *BPJS Ketenagakerjaan* is crucial considering the large amount of sensitive information collected, such as NIK, account number, salary data, and family information. BPJS Employment as a public legal entity responsible for the social security program for workers is required to comply with the provisions of personal data protection in accordance with Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).

At the Denpasar Branch Office, the implementation of data protection is carried out through internal procedures that refer to the basic principles of the PDP Law such as the principles of transparency, specific objectives, data minimization, and data security. The implementation of the participant information system uses technology that is integrated with cybersecurity in accordance with Presidential Regulation No. 39 of 2019 concerning One Data Indonesia, as well as the provisions of BPJS Employment Regulation No. 1 of 2021 concerning Participant Data and Information Governance.

However, in practice, there is still potential for data leakage through the misuse of internal access, weak verification controls in the online system, and a lack of education among participants about the right to personal data. Therefore, strengthening legal protection mechanisms should involve:

1) Periodic audits of IT systems and data management HR.
2) External supervision by the Information Commission and the personal data protection authority (PDP Authority).
3) Improving digital literacy for participants related to rights and complaints mechanisms for data breaches

The management of personal data in *BPJS Ketenagakerjaan* membership is closely related to the right to legal protection as guaranteed in the constitution and laws and regulations. At the Denpasar Branch Office, *BPJS Ketenagakerjaan* collects and processes various participant information, such as personal identity, contact information, employment data, and contribution payment history. All of this data belongs to the category of personal data, which according to Article 1 number 1 of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), is part of the private rights of individuals that must be protected by the state.

In the perspective of legal protection theory, as stated by Philipus M. Hadjon, legal protection is any effort given to legal subjects to obtain justice, including preventive and repressive protection from the arbitrary actions of other parties, especially the government or public institutions. In this context, BPJS participants as legal subjects must be given assurances that their personal data will not be misused, disseminated, or accessed without lawful permission.

Preventively, *BPJS Ketenagakerjaan* has an obligation to apply data processing principles such as accountability, fairness, transparency, and purpose restrictions as stipulated in the PDP Law. This must be realized through internal privacy policies, digital system security, and participant education regarding the rights to their personal data. For example, the Denpasar Branch Office has started implementing two-step encryption and verification procedures in the online claims system. However, the effectiveness of its implementation still faces challenges, such as limited digital literacy of participants and potential misuse of internal access.

In the event of repression, legal protection can be carried out in the event of a leak or misuse of personal data. Participants have the right to submit objections or reports to BPJS or the Personal Data Protection Authority (OPDP). Unfortunately, according to the results of research by Yulianti, most public institutions, including BPJS, have not been optimal in providing complaint channels and mechanisms for resolving personal data disputes in a transparent manner.

At the implementation level, legal arrangements related to the protection of personal data in the implementation of social security by *BPJS Ketenagakerjaan* are supported by two main frameworks: first, Law Number 24 of 2011 concerning BPJS which requires social security providers to maintain the confidentiality of participant data; and second, the PDP Law of 2022 which regulates the principles and obligations of data controllers, including BPJS as a public legal entity. Important principles in the relevant PDP Law applied by BPJS include the principles of transparency, purpose limitation, security, accountability, and fairness in the processing of personal data. Social security providers are obliged to ensure that participant data is used only for legitimate purposes, is not disseminated to third parties without permission, and is stored in a secure system.

However, in practice, legal protection of the personal data of BPJS participants at the regional level, including at the Denpasar Branch Office, still faces several structural and

technical challenges. A study by Lestari and Sudarma (2023) shows that there is still a lack of understanding of personal data rights among participants, weak transparency in providing information related to data management, and the lack of optimal security of the digital systems used by *BPJS Ketenagakerjaan*. This strengthens the need for an active role of BPJS as a data controller to provide effective educational facilities, information services, and complaint mechanisms for participants.

In addition, legal protection also needs to touch on the repressive aspect. In the event of a violation—such as data leakage, misuse of internal access, or provision of data to a third party without legal basis—the participant has the right to file a lawsuit, either administratively to the data supervisory institution (OPDP) or civilly in court. Unfortunately, according to Yulianti (2021), the system of supervision and sanctions for data violations within state institutions has not run optimally, due to the lack of a strong independent supervisory institution and the limitations of the implementation of administrative sanctions in the PDP Law.

In the context of legal protection at the *BPJS Ketenagakerjaan* Denpasar Branch Office, a preventive approach must be realized in the form of strong internal policies, employee training on personal data governance, strengthening information systems based on end-to-end encryption, and regular information technology audits. On the other hand, a repressive approach can be implemented through the provision of public complaint channels and clarity of the mechanism for handling data breaches. Collaboration with the Ministry of Communication and Informatics and the Personal Data Protection Authority is also needed to build a legal system that is responsive and adaptive to the development of digital technology.

Thus, the theory of legal protection plays an important role as a philosophical and normative foundation for the state in providing legal certainty, justice, and a sense of security to every citizen. Legal protection of personal data in social security participation is not only the responsibility of the institution, but is part of the state's commitment to protecting dignity and human rights in the digital era.

In addition to the PDP Law, legal protection of personal data in the context of public services such as BPJS can also be seen from the perspective of Law Number 25 of 2009 concerning Public Services, which requires service providers to respect the rights of service users, including the protection of personal information. In this case, the Denpasar Branch of BPJS Employment Office has a dual obligation: maintaining service quality and ensuring the protection of all personal information collected in its system.

With the increasing dependence on digital systems, the protection of personal data in BPJS membership has become crucial. Therefore, there is a need for synergy between strong regulations, a transparent internal supervision system, and participant literacy so that legal protection of personal data is not only a formality, but truly part of a social security system that respects human dignity and rights.

Considering the complexity of the data managed and the status of *BPJS Ketenagakerjaan* as a public legal entity, the legal protection arrangements for participants' personal data, especially at the Denpasar Branch Office, must be implemented comprehensively and continuously. This arrangement is not only normative through Law Number 27 of 2022 concerning Personal Data Protection and Law Number 24 of 2011 concerning BPJS, but also needs to be realized operationally through internal policies that prioritize the principles of accountability, transparency, and participant participation. The

implementation of personal data protection at the branch level must pay attention to the technical aspects of information security, internal access restrictions, legal education for employees, and the provision of effective complaint channels. Therefore, legal protection of personal data in *BPJS Ketenagakerjaan* membership is not only an administrative aspect, but is a tangible manifestation of the fulfillment of citizens' constitutional rights to privacy, which demands legal responsibility, service professionalism, and public supervision on an ongoing basis.

Legal Responsibility of *BPJS Ketenagakerjaan* Denpasar Branch in Protecting Participants' Personal Data

In the era of digitization of public services, the protection of participants' personal data is a crucial aspect that must be fulfilled by every social security provider, including *BPJS Ketenagakerjaan*. As a public legal entity, *BPJS Ketenagakerjaan* Denpasar Branch has a legal responsibility to maintain the confidentiality and security of the personal data of all its participants. This is in line with the provisions in Law Number 27 of 2022 concerning Personal Data Protection, which requires every data controller to protect personal information from misuse, illegal access, and data leakage. Thus, the legal responsibilities inherent in *BPJS Ketenagakerjaan* Denpasar Branch not only include administrative and technical aspects, but also part of efforts to protect human rights in the field of employment.

As a branch of the central agency, *BPJS Ketenagakerjaan* Denpasar implements national policies and guidelines related to the management of participant data. In practice, this branch is responsible for overseeing the process of collecting, storing, and distributing data in an accountable manner, including ensuring that every employee who accesses the participant's information system has received special training on confidentiality and data protection ethics. This effort is carried out to avoid potential violations of the law and ensure the fulfillment of data protection principles as stipulated in Articles 20 to 34 of the PDP Law.

In addition, *BPJS Ketenagakerjaan* Denpasar Branch is also required to provide a complaint mechanism that can be used by participants when they feel that their data rights are violated. Actions such as granting unauthorized access, leaking medical or financial information, and data processing without valid consent may be subject to administrative criminal sanctions as stated in the sanction’s provisions of the PDP Law. In this context, the Denpasar branch is not only internally responsible to the head office, but also legally to the participants as data subjects.

Thus, the protection of personal data within *BPJS Ketenagakerjaan* Denpasar Branch is an integral part of its legal responsibilities as a public service provider. Compliance with laws and regulations, the implementation of information security systems, and strengthening the capacity of human resources are the main pillars in carrying out this obligation optimally and sustainably.

As an employment social security provider, *BPJS Ketenagakerjaan* Denpasar Branch has a legal responsibility to protect participants' personal data as stipulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). In the regulation, BPJS acts as a controller of personal data that is obliged to ensure that every process of data collection, storage, use, and deletion is carried out in accordance with the principles of personal data protection, such as validity of the purpose, access restrictions, transparency, and accountability.

This responsibility is technically translated into several concrete steps in the Denpasar Branch, including through the implementation of information technology-based security systems, such as data encryption, internal access restrictions, and periodic audits of personnel and participant information systems. In addition, *BPJS Ketenagakerjaan* Denpasar is also active in socializing and educating participants and employers regarding the importance of personal data protection, as has been carried out through public discussion forums and training on new regulations on social security and worker protection.

In the operational context, the legal responsibility of the Denpasar branch is strengthened through central policies and internal regulations of BPJS, such as the data confidentiality policy and data leak incident reporting protocol. In the event of a violation or data leak, legal liability can lead to administrative sanctions as stipulated in Articles 57 to 60 of the PDP Law, and even civil lawsuits based on Article 1365 of the Civil Code regarding unlawful acts.

BPJS Ketenagakerjaan as a public legal entity established based on Law Number 24 of 2011 concerning the Social Security Administration Agency, has the main function of organizing the employment social security program. In carrying out its functions, BPJS collects and manages various participants' personal data, which includes identity data, employment data, health data, and financial data. Along with the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), *BPJS Ketenagakerjaan*, including the Denpasar Branch Office, juridically assumes the responsibility as a data controller who must ensure the security, confidentiality, and integrity of participants' personal data.

In the context of legal responsibility, these obligations are not purely normative, but have juridical consequences if ignored or violated. According to legal liability theory, any legal subject who commits an unlawful act—either intentional (culpa lata) or negligence (culpa levis)—can be held administratively, civilly, or criminally, depending on the form of the violation. In this case, if *BPJS Ketenagakerjaan* Denpasar Branch is negligent in carrying out personal data protection obligations, such as data leakage due to system weaknesses, unauthorized access by employees, or misuse of data by third parties, then this institution can be held legally liable according to the provisions in Articles 58-60 of the PDP Law.

BPJS Ketenagakerjaan Denpasar Branch's legal obligations in protecting participants' data are reflected in various concrete actions, such as the implementation of technology-based security systems (including encryption, firewalls, and double authentication), internal access rights restrictions, training for data service officers, and the establishment of internal policies regarding information governance and data confidentiality. On the other hand, there is also an obligation to provide a complaint channel and a mechanism for redressing rights for participants who feel aggrieved by personal data breaches. This is in line with the principle of accountability in the theory of accountability, namely that the party who is given authority is also obliged to account for all consequences of the use of this authority, especially if it causes losses to other parties.

The application of the theory of legal liability in the context of personal data protection by *BPJS Ketenagakerjaan* Denpasar Branch also reflects the principle of strict liability in modern administrative law, where liability does not always have to be proven by fault-based liability, but simply by proving that legal obligations are not carried out as they should. For example, if there is a data breach that can be proven to be caused by negligence of the security

system, then the participant has the right to demand liability without the need to prove intentionality from BPJS as the data controller.

Furthermore, in the theory of Indonesian civil law, such liability can be categorized as an unlawful act (*onrechtmatige daad*) as referred to in Article 1365 of the Civil Code (KUHPerdata), which states that "every unlawful act, which brings harm to another person, obliges the person who by his fault publishes the loss to compensate for the loss." So, if negligence in maintaining data confidentiality causes material or immaterial losses to participants, *BPJS Ketenagakerjaan* Denpasar Branch can be sued civilly through a compensation lawsuit mechanism.

In addition to the civil aspect, BPJS can also be subject to administrative sanctions by supervisory institutions such as the Ministry of Communication and Information, as stipulated in Articles 57 to 59 of the PDP Law. These sanctions can be in the form of written reprimands, administrative fines, temporary suspension of data processing activities, and data deletion. In more serious cases, such as if there is an illegal dissemination of personal data, the violation can be charged with criminal sanctions as referred to in Articles 67 to 73 of the PDP Law.

Thus, the legal responsibility of *BPJS Ketenagakerjaan* Denpasar Branch in protecting participants' personal data is multi-dimensional: including administrative responsibility (in the form of compliance with regulations), civil liability (if losses arise for participants), and criminal liability (if there is an element of intentionality or neglect of violations of the law). All these responsibilities are rooted in the principle of *lex specialis derogat legi generali*, where the PDP Law applies specifically to the control of personal data, complementing the general provisions in state administrative law, civil law, and criminal law.

The legal responsibilities of *BPJS Ketenagakerjaan* Denpasar Branch are also reflected in the institution's obligation to comply with the general principles of personal data processing as mentioned in Article 20 of the PDP Law, such as the principles of purpose validity, purpose limitation, data minimization, accuracy, integrity and confidentiality, and accountability. This emphasizes that the process of collecting and deleting data must be carried out in a legal, transparent, and accountable manner. For example, if the Denpasar Branch Office collects worker data without an adequate explanation of the purpose of its use or disseminates the data to a third party without a clear legal basis, then this action can be classified as a violation of the law.

In practice, *BPJS Ketenagakerjaan* Denpasar Branch has taken various preventive measures, such as the use of technology-based information systems equipped with data security features (encryption, access control, and firewall), internal training for service staff, and the implementation of information security policies. However, technical steps alone are not enough. Legal responsibility requires BPJS to also establish internal and external supervision mechanisms. Internally, BPJS must have regular audit procedures and protocols for handling data breach incidents. Externally, BPJS is obliged to open access to complaints for participants and cooperate with supervisory authorities, such as *Kominfo* or OJK, in the event of a violation.

Another important aspect is the recognition and protection of the rights of personal data subjects, which according to the PDP Law includes the right to obtain information, the right to access and correct data, the right to withdraw consent, the right to delete data, as well as the right to demand compensation. The Denpasar Branch Office must provide easy and responsive access to participants to exercise these rights. Negligence in providing this means can be

considered a violation of administrative law, which can lead to sanctions as stipulated in Article 57 of the PDP Law, ranging from written reprimands to temporary suspension of data processing activities.

From a civil law perspective, if negligence in protecting personal data results in losses for participants, then this can be qualified as an unlawful act (*onrechtmatige daad*) based on Article 1365 of the Civil Code. In this case, the participant who feels aggrieved has the right to claim damages based on violation of the right to privacy or the leakage of personal information. For example, if participant data is leaked and used by a third party for fraud or defamation, BPJS can be sued civilly for not being able to meet its inherent protection obligations.

Meanwhile, in the criminal law aspect, the PDP Law also stipulates that misuse or leakage of personal data carried out deliberately, such as selling or disseminating personal data without permission, can be subject to criminal sanctions of imprisonment or fines. If it is proven that there is an element of fatal negligence on the part of the system manager or BPJS officer, then the individual perpetrator or person in charge of the institution can also be subject to additional penalties. Therefore, BPJS's legal responsibility is not only institutional, but can also be personally attached to officials or employees who are proven to be negligent.

Furthermore, the implementation of the legal responsibilities of *BPJS Ketenagakerjaan* Denpasar Branch must also be associated with the principles of good governance and transparency of public services. As a public body that manages participant funds, BPJS is obliged not only to be transparent in terms of finances and social security benefits, but also in the governance of participant data. Public trust in BPJS is highly determined by how much this institution can maintain data security and confidentiality as a form of protection of citizens' constitutional rights to privacy.

Thus, *BPJS Ketenagakerjaan* Denpasar Branch has a comprehensive legal responsibility in protecting participants' personal data, which includes administrative, civil, criminal, and ethical liabilities. The implementation of this responsibility cannot be separated from the principles of the rule of law and the supremacy of human rights, especially the right to a sense of security in using digital-based public services. Failure to fulfill this responsibility will have an impact not only legally, but also on the reputation of the institution and the effectiveness of the social security system.

In addition to being based on Law Number 27 of 2022 concerning Personal Data Protection, the legal responsibility of *BPJS Ketenagakerjaan* Denpasar Branch is also supported by a number of other sectoral regulations that strengthen data protection obligations. Among them are Law Number 24 of 2011 concerning BPJS, Presidential Regulation Number 109 of 2013 concerning the Establishment of Social Security Program Participation, and Regulation of the Minister of Manpower and Transmigration related to the implementation of social security programs. In all these regulations, there is an implicit and explicit mandate that participant data is an integral part of social security services and must be maintained to ensure the continuity of participants' rights.

This is important because failure to protect personal data not only has implications for individual participants, but can also undermine the integrity of the social security system itself. For example, if membership data is leaked into the hands of irresponsible parties, there can be fraud in benefit claims, falsification of payroll data, and manipulation of employment status which ultimately harms the state and society. Therefore, BPJS's legal responsibility is not

solely reactive, but proactive in building a system for prevention and early detection of potential data breaches.

From the point of view of consumer protection legal theory, BPJS participants can also be positioned as consumers of public services. In this context, the principle of duty of care must be fully implemented by *BPJS Ketenagakerjaan* Denpasar Branch. This principle confirms that public service providers are obliged to carry out their duties with a certain degree of care, especially in matters that can cause losses, such as the management of sensitive information. If this principle is ignored, and losses are incurred by the participant, then liability can be legally enforced, even without having to prove the existence of malicious intent (*mens rea*).

In the context of information technology-based public services, *BPJS Ketenagakerjaan* Denpasar Branch is also required to comply with electronic system standards as stipulated in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This PP requires every electronic system operator (PSE), including government agencies, to ensure the security, integrity, availability, and confidentiality of managed electronic information. Failure to meet this standard can cause BPJS to be considered legally negligent and prosecuted both administratively and civilly.

Furthermore, BPJS's legal responsibility also concerns the aspect of institutional ethics, namely the moral responsibility to maintain public trust as a state service entity. In this case, *BPJS Ketenagakerjaan* Denpasar Branch is not only a technical operator of the social security program, but must also carry out its function as a human rights guardian for the privacy and security of personal information. This institutional ethics is important because in many data breach cases, reputational damage is often more severe than the legal sanctions imposed.

Strengthening BPJS's legal responsibility can also be done through public accountability mechanisms, for example through external audits by independent supervisory agencies, publication of personal data protection policies, and the involvement of public participation in monitoring service systems. This is in line with the principles of good governance which emphasize openness, responsibility, and participation as the foundation in managing public services.

In terms of jurisprudence, although until now there have not been many data leak cases filed against *BPJS Ketenagakerjaan* specifically, several legal precedents related to personal data in the public service sector can be used as a reference to assess the extent to which legal responsibility can be imposed on state institutions. In many court rulings, the principle of "the data controller is responsible for any negligence that causes loss" is the main basis for the imposition of sanctions.

The legal principles of personal data protection carried out by *BPJS Ketenagakerjaan* Denpasar Branch cannot be separated from the influence of international legal norms that have begun to be adopted in the national legal system. For example, in the General Data Protection Regulation (GDPR) that applies in the European Union, there are fundamental principles such as lawfulness, fairness, and transparency, purpose limitation, data minimization, and storage limitation, which are also adopted in the Indonesian PDP Law. Thus, BPJS *Ketenagakerjaan*'s legal responsibility in protecting participants' personal data is not only national, but also reflects global protection standards that place the right to privacy as part of universal human rights.

In this framework, the legal responsibility is not only to comply with the regulations, but also to ensure a sense of security and legal certainty for the participants. At the operational

level, the Denpasar Branch Office needs to build a privacy management system that integrates the three main pillars of data protection:

1) Clear and written internal policies;
2) Strong and tested information technology; and
3) Human resources who are trained and understand data protection ethics.

Without the synergy of these three elements, legal responsibility tends to be just an administrative formality with no real functioning.

Furthermore, in the aspect of supervision and law enforcement, it is also important to consider the role of independent supervisory institutions. The PDP Law has mandated the establishment of the Personal Data Protection Authority (OPDP) which will later be responsible for supervising the implementation of data protection throughout Indonesia. Until this institution is formed functionally, the temporary supervisory role is carried out by the Ministry of Communication and Information Technology (*Kominfo*). The Denpasar Branch Office, as an operational unit, must establish an intensive coordinating relationship with the Regional Communication and Informatics, BSSN (State Cyber and Cryptography Agency), and the Regional Government in responding to potential data security incidents or complaints from participants.

To strengthen the implementation of its legal responsibilities, *BPJS Ketenagakerjaan* Denpasar Branch can also form a data protection task force that is specifically tasked with conducting periodic audits, reviewing internal privacy policies, handling participant complaints, and providing technical and procedural recommendations to branch leaders. The establishment of this task force can function as a self-regulation mechanism that prioritizes compliance and early prevention of violations of the law.

More than that, increasing people's digital literacy is also an important factor in the success of personal data protection. The legal responsibility of *BPJS Ketenagakerjaan* Denpasar Branch in this context is not only internal, but also external in the form of education and socialization to participants regarding their rights to personal data. This can be done through counseling to participating companies, partners, and informal worker groups in the Denpasar area. This education is very important to avoid public ignorance of data protection, which can be used by individuals to commit fraud, falsification claims, or data manipulation.

As for prospectively, the implementation of legal responsibilities in the field of personal data protection must also consider future technological developments, including the use of artificial intelligence (AI), big data, and cloud computing systems. BPJS's dependence on this technology will be even greater, so dynamic and adaptive policies are needed so that the system is not only efficient, but also legally safe. The Denpasar Branch Office, in this case, must be a pioneer in the implementation of digital security standards that are responsive to these developments, without sacrificing the basic rights of participants.

Finally, it is necessary to realize that the protection of personal data is not only a legal responsibility, but also part of the social responsibility of public institutions towards the communities they serve. In the legal relationship between participants and BPJS, there is a fiduciary relationship, where participants entrust their sensitive data to state institutions. Therefore, a violation of this principle not only creates legal consequences, but can also undermine the foundations of public trust. In this case, *BPJS Ketenagakerjaan* Denpasar Branch must show real commitment, not only in the form of regulations, but also in the form

of concrete actions that prove that personal data protection is part of excellent service that is dignified and legally responsible.

Thus, *BPJS Ketenagakerjaan* Denpasar Branch has a comprehensive legal responsibility in maintaining the protection of participants' personal data, both from normative, structural, and technical operational aspects. This obligation is not only based on national laws and regulations such as Law Number 27 of 2022 concerning Personal Data Protection, but is also based on the principles of prudence, accountability, and public service ethics. From the perspective of legal liability theory, BPJS is not only responsible when there is a violation of the law due to error, but can also be held accountable for negligence in preventing such violations. Therefore, to realize effective personal data protection, the Denpasar Branch Office must consistently integrate privacy policies, strengthen information security systems, increase human resource capacity, and educate participants as a tangible form of the institution's commitment to protecting people's digital rights.

CONCLUSION

The regulation of personal data protection in *BPJS Ketenagakerjaan* Denpasar Branch membership upholds citizens' privacy rights, with the institution serving as data controller obligated to collect, store, and process data legally, securely, and transparently under Law Number 27 of 2022 concerning Personal Data Protection and Law Number 24 of 2011 concerning the Social Security Administering Agency. Despite this framework, implementation challenges persist, including limited human resources, suboptimal security systems, and participants' limited awareness of rights, exposing *BPJS Ketenagakerjaan* to administrative, civil, and criminal liability for negligence. This underscores not only formal obligations but also ethical responsibilities to sustain public trust in social security. Strengthening data systems, internal training, and participant education is essential for accountability. Future research could empirically assess the effectiveness of these measures through comparative case studies across *BPJS* branches nationwide.

REFERENCES

Alfitri, N. A., Rahmawati, R., & Firmansyah, F. (2024). Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Journal Social Society*, *4*(2). https://doi.org/10.54065/jss.4.2.2024.511

Andriana Putri, N. (2023). Doxing untuk Malicious Purposes vs Doxing untuk Political Purposes: Urgensi Pengklasifikasian Ancaman Hukuman Bagi Para Pelaku Doxing dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Padjadjaran Law Review*, *11*(1). https://doi.org/10.56895/plr.v11i1.1286

Anissa, S., & Multazam, M. T. (2024). Assessing Legal Measures for Addressing Personal Data Misuse in Commercial Settings: A Critical Analysis. *Indonesian Journal of Law and Economics Review*, *19*(2). https://doi.org/10.21070/ijler.v19i2.1012

Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2025). Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia). *Jurnal Multidisiplin Ilmu Akademik*, *2*(1).

Bratina, T. (2023). Digital Devices And Interpersonal Communication Over Time. *Journal of Elementary Education*, *16*(4). https://doi.org/10.18690/rei.2958

Chong, M. T., Puah, C. H., & Teh, C. S. (2025). Digital policy initiatives and infrastructure in Malaysia: driving economic and financial growth through the Digital Economy Performance Indicator. *International Journal of Social Economics*. https://doi.org/10.1108/IJSE-10-2024-0826

Febrian, F., Saputra, I. Y., & Napitupulu, D. R. W. (2025). Implikasi Hukum terhadap Perlindungan Data Pribadi dalam Transaksi Fintech. *Rechtsnormen Jurnal Komunikasi Dan Informasi Hukum*, *4*(1). https://doi.org/10.56211/rechtsnormen.v4i1.1153

Ichhpujani, P., Singh, R. B., Foulsham, W., Thakur, S., & Lamba, A. S. (2019). Visual implications of digital device usage in school children: A cross-sectional study. *BMC Ophthalmology*, *19*(1). https://doi.org/10.1186/s12886-019-1082-5

Kaewunruen, S., Sresakoolchai, J., Ma, W., & Phil-Ebosie, O. (2021). Digital twin aided vulnerability assessment and risk-based maintenance planning of bridge infrastructures exposed to extreme conditions. *Sustainability*, *13*(4), 2051.

Ketmaneechairat, H., Maliyaem, M., & Puttawattanakul, P. (2024). Towards a Management System Framework for the Integration of Personal Data Protection and Data Governance: A Case Study of Thai Laws and Practices. *International Journal of Technology*, *15*(1). https://doi.org/10.14716/ijtech.v15i1.5885

Muharom, F., Nugroho, A., & Putra, H. R. P. (2022). Self-directed Use of Digital Devices for Out-of-class English Learning. *International Journal of Education in Mathematics, Science and Technology*, *10*(1). https://doi.org/10.46328/ijemst.2245

Osmundsen, K., & Bygstad, B. (2022). Making sense of continuous development of digital infrastructures. *Journal of Information Technology*, *37*(2). https://doi.org/10.1177/02683962211046621

Prabowo, O. M., Mulyana, E., Nugraha, I. G. B. B., & Supangkat, S. H. (2023). Cognitive City Platform as Digital Public Infrastructure for Developing a Smart, Sustainable and Resilient City in Indonesia. *IEEE Access*, *11*, 120157–120178.

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1). https://doi.org/10.38043/jah.v8i1.6793

Saurabh, S. (2024). The Digital Personal Data Protection Act Of 2023: Strengthening Privacy In The Digital Age. *International Journal of Law in Changing World*, *3*(2). https://doi.org/10.54934/ijlcw.v3i2.84

Siahaan, I. R., Sipayung, R. N., Lita, I., Zahra, Q., Naseela, I., Hanny, H., & Rakhmawati, N. A. (2024). Analisis Praktik Perlindungan Data Pribadi pada Aplikasi 'Satusehat terhadap Regulasi Hukum di Indonesia. *Jurnal Teknoinfo*, *18*(1).

Tømte, C. E. (2024). Conceptualisation of professional digital competence for school leaders in schools with 1:1 coverage of digital devices. *Computers and Education*, *222*. https://doi.org/10.1016/j.compedu.2024.105151

Wang, L., & Shao, J. (2024). The energy saving effects of digital infrastructure construction: Empirical evidence from Chinese industry. *Energy*, *294*. https://doi.org/10.1016/j.energy.2024.130778