Journal of International Islamic Law, Human Rights, and Public Policy
(JISHUP Journal) | ISSN(e): 3031-2280
Website https://jishup.org/index.php/ojs/index | Volume 4 No. 3 (2026)

RECONSTRUCTION OF ARTICLE 34 OF THE LAW ON GENERAL PROVISIONS AND TAX PROCEDURES (KUP LAW) ON THE GOVERNANCE OF THE ACCOUNTABILITY OF THE DIRECTORATE GENERAL OF TAXES FOR THE MISUSE OF DIGITAL IDENTITY IN THE E-FAKTUR SYSTEM

Natalia Ratih Jatmikani[1] Ariy Khaerudin[2] Femmy Silaswaty[3]
[1,2,3]Universitas Islam Batik Surakarta
ratihjatmikani3500@gmail.com

Received: 03/06/2026 | **Revised:** 08/06/2026 | **Accepted:** 20/06/2026 | **Published:** 11/07/2026

Abstract

Digital-based tax services require the Directorate General of Taxes to maximize the protection of personal data in the form of digital taxpayer identities, such as the Population Identification Number (KIP), which is currently used as the Taxpayer Identification Number. The purpose of this research is to analyze the reconstruction of Article 34 of the General Provisions of Taxation Law concerning the governance of the Directorate General of Taxes' accountability for the misuse of digital identities in the system.and-Invoices. The study was conducted using a normative method with a statutory and conceptual approach. The data used was secondary data collected through literature review and analyzed qualitatively and descriptively. The results indicate that there are no laws and regulations specifically governing the Directorate General of Taxes' accountability in the event of misuse of digital identities within the system.and-Invoices because so far the form of prohibition regulated is limited to the dissemination of personal data by officials without affecting electronic systems. Therefore, it is necessary to reconstruct Article 34 of the General Provisions of Taxation Law by adopting the provisions in Article 47 of the Personal Data Protection Law, which places the Directorate General of Taxes as the controller of personal data in both conventional and digital forms, thereby providing certainty and legal protection for taxpayers. Forms of accountability that can be added include administrative sanctions and criminal sanctions for any form of possible data leaks that are not caused by the error or negligence of tax officials.

Keywords: e-Facture, digital identity, responsibility, governance

INTRODUCTION

Electronic tax services are one form of improvement in tax administration intended to provide convenience for taxpayers. These electronic-based services began to be implemented in various sectors of life following the issuance of Presidential Regulation Number 95 of 2018 concerning the Electronic-Based Government System. In addition to providing convenience for the public as users, the electronic-based taxation system administered by the Directorate General of Taxes is also intended to reduce the workload of tax officials and minimize the risk of human error in the provision of tax services.(Wange & Katili, 2024)

In 2023, the Directorate General of Taxes (DJP) introduced a new policy by designating the National Identity Number (Nomor Induk Kependudukan/NIK) as the Taxpayer Identification Number (Nomor Pokok Wajib Pajak/NPWP). The NPWP is an official number issued by the DJP when a person has fulfilled the requirements as a taxpayer. Before the use of the NIK format as the NPWP, the NPWP consisted of a combination of random numbers issued by the DJP. The designation of the NIK as the NPWP is based on Article 2 paragraph (1a) of Law Number 7 of 2021 concerning the Harmonization of Tax Regulations, which states that: “The Taxpayer Identification Number as referred to in paragraph (1) for individual taxpayers who are residents of Indonesia shall use the National Identity Number.” The reason behind this policy is to realize “One Data Indonesia” in order to create integration and standardized equality in every administrative service, including tax administration. In addition, the conversion of the NIK into the NPWP is expected to simplify and improve the efficiency and effectiveness of the DJP in tax administration.(Melani & Doloksaribu, 2024) The use of the NIK as the NPWP, on the one hand, provides convenience in terms of data integration. On the other hand, it creates new legal implications related to the protection of taxpayers' digital identities. Initially, the NIK functioned only as population data, which constitutes specific personal data owned by every Indonesian citizen. However, once the NPWP was assigned the same identification number as the NIK, the NIK also became an instrument for accessing various digital tax services administered by the DJP. This similarity creates a greater risk of misuse because when the NIK is known by another person and used without authorization, the person misusing it can also access the taxpayer's tax administration.(Ardin, 2022)

One electronic tax administration system closely related to the use of digital identities such as the NPWP is the electronic tax invoice (e-Faktur) system. The definition of a tax invoice is regulated in Article 1 point 23 of Law Number 42 of 2009 concerning the Third Amendment to Law Number 8 of 1983 concerning Value Added Tax on Goods and Services and Sales Tax on Luxury Goods, as last amended by Law Number 7 of 2021, which states that: "A Tax Invoice is proof of tax collection made by a Taxable Entrepreneur who delivers Taxable Goods or Taxable Services." The e-Faktur system facilitates the preparation and/or reporting of tax invoices. In addition, the electronic system improves the effectiveness of supervision and the transparency of tax transactions.(Indriastuti et al., 2025)

When a company first registers with the DJP to be confirmed as a Taxable Entrepreneur (Pengusaha Kena Pajak/PKP), the PKP is required to immediately apply for an Electronic Certificate, which will subsequently be used to access the e-Faktur application for issuing tax invoices. The Electronic Certificate contains the NPWP as the primary digital identity. In addition to the NPWP, it also contains the taxpayer's name, public key, and the certificate validity period, all of which constitute the taxpayer's digital identity. If the Electronic Certificate is compromised, the digital identity contained therein is clearly at high risk of misuse.(Utami & Abd, 2024)

The leakage of taxpayers' digital data may be caused by several factors, including hacking or phishing by external parties as one of the risks associated with the use of information technology in service delivery. In addition, data leakage may also result from the internal misuse of personal data by DJP officials or employees who have full access to the Electronic Certificate portal. When the digital data contained in the Electronic Certificate is leaked, unauthorized parties may create fictitious e-Faktur in the name of the PKP, even though the PKP has never carried out the transactions stated in the e-Faktur. This situation is again caused by the leakage of digital data, such as the NPWP contained in the Electronic Certificate, where the certificate is intended for the creation of e-Faktur.(Siregar et al., 2024)

Invoices issued in electronic form naturally contain taxpayers' identities that have been integrated into the national tax system. On the one hand, this offers efficiency in terms of time, cost, and process. On the other hand, it creates opportunities for the misuse of digital identities, including the use of the NIK by other parties without lawful authority in the process of issuing electronic tax invoices. The misuse of the NIK may result in tax obligations that were never actually incurred, as well as the risk of tax crimes. Taxpayers whose NIK has been misused must prove that the transactions stated in the invoice were never carried out by them.(Utami & Abd, 2024)

The regulation concerning the protection of taxpayers' personal data remains very limited under Law Number 6 of 1983 concerning General Provisions and Tax Procedures (KUP Law), as amended by Law Number 7 of 2021, because there is no provision governing the legal protection that may be provided by the Directorate General of Taxes (DJP), as the operator of the electronic tax system, to taxpayers whose personal data has been misused by other parties. To date, the existing regulations focus only on taxpayers' administrative compliance and do not regulate legal protection for taxpayers who become victims of the misuse of personal data such as the NPWP.(Nurmala & Wiraguna, 2026)

The regulation concerning the DJP's responsibility for data breaches is stipulated in Article 34 paragraph (1) of the KUP Law, which states that: "Every official is prohibited from disclosing to any other party anything known to or informed to him or her by a Taxpayer in the course of his or her office or duties for the implementation of the provisions of laws and regulations." From this provision, it is evident that the data breach risk accommodated by the KUP Law is limited to disclosures made by officials as internal employees. In the e-Faktur issuance system, however, the risk of data breaches arises not only from internal officials but also from phishing or hacking, which may result in the NIK (NPWP) as a digital personal identity becoming known to and misused by other parties. The KUP Law does not regulate the DJP's responsibility where NPWP data breaches occur due to phishing or hacking.

To address the gap in personal data protection, the Government enacted Law Number 27 of 2022 concerning Personal Data Protection, which designates the DJP as a "Personal Data Controller." The DJP's responsibility as a Personal Data Controller for personal data protection is clearly regulated in Article 47 of the Personal Data Protection Law, which states that: "A Personal Data Controller shall be responsible for the processing of Personal Data and shall demonstrate accountability in fulfilling its obligations to implement the principles of personal data protection."

In practice, however, the KUP Law has not provided clear regulations regarding the forms of protection and accountability that may be provided by the DJP concerning the misuse of electronic personal data in the e-Faktur system, as its provisions remain limited to administrative and conventional service purposes.

Therefore, the Personal Data Protection Law plays an important role in providing protection for personal data, even though Article 74 of the Law provides that: "Upon the entry into force of this Law, Personal Data Controllers, Personal Data Processors, and other parties related to the processing of personal data shall comply with the personal data processing provisions under this Law no later than 2 (two) years after this Law is promulgated." This means that by 2024 at the latest, the KUP Law and Law Number 7 of 2021 should have been aligned with the regulations on electronic personal data protection, although in reality such regulations have not yet been established.(Primayudhana, 2025)

Based on these issues, legal reconstruction is necessary to harmonize the existing laws and regulations, particularly regarding the governance of the DJP's accountability in administering the e-Faktur system, so that the DJP is responsible not only for administrative matters but also for providing legal protection to digital identity holders. In light of these issues, this study is considered necessary, with its primary focus on examining the governance of the DJP's accountability concerning the misuse of digital personal data in the e-Faktur system.

LITERATURE REVIEW

The first theory used in this study is the welfare state theory proposed by Jeremy Bentham, which states that the state, through the government, is responsible for ensuring "the greatest happiness of the greatest number of its citizens.(Pamungkas & Hariri, 2022)" Bentham argued that the measure of happiness arises when citizens can experience the benefits of what is offered by the government because the orientation of government policy is to provide happiness for its citizens. In relation to the issue of tax digital data protection, this falls within the authority of the Directorate General of Taxes as the organizer representing the state in carrying out its functions, and when tax services fail to provide benefits and happiness to the public, the DJP must be held accountable.

The second theory is the theory of personal data protection. Personal data may generally be defined as information used to identify an individual, either directly or indirectly, such as a name, identification number, location data, or biometric facial recognition data. From a linguistic perspective, the Indonesian Dictionary (Kamus Besar Bahasa Indonesia) defines personal data as "data relating to a person's characteristics, such as name, age, gender, education, occupation, address, and position within the family."(Sugono, 2018) Personal data in the field of taxation includes taxpayers' identities and the NPWP, which has now been integrated with the NIK. Personal data protection also applies when such data is in digital form, as used in the e-Faktur tax system. Such protection is classified into two forms, namely preventive protection, which is carried out through the fulfillment of taxpayers' rights relating to their digital identities, and repressive protection, which functions to resolve cases involving the misuse of digital identities. In order to provide legal protection, there must be statutory regulations governing the matter so as to provide legal certainty not only for taxpayers but also for tax administrators, enabling each party to understand its respective rights, obligations, and prohibitions according to its legal position.

METHOD

The type of research used in this study is normative legal research, which assesses the validity of law conceptually by referring to the positive legal system. In other words, it examines legal issues from the perspective of das sollen, evaluating law as an ideal system of values.(Tan, 2021) The nature of this research is explanatory research because its focus is to reconstruct the regulation concerning the governance of the accountability of the Directorate General of Taxes. Therefore, it not only describes and analyzes the existing regulations but also examines the causal relationship between the misuse of taxpayers' digital personal data and the gaps in the accountability of the Directorate General of Taxes concerning the misuse of the e-Faktur system.

The research employs two approaches, namely the statutory approach and the conceptual approach. The statutory approach is conducted by examining all written regulations relevant to the issues under analysis. Meanwhile, the conceptual approach relies on theories, concepts, or doctrines developed by legal scholars. In this study, the type of data used is secondary data, consisting of primary, secondary, and tertiary legal materials. The secondary data were collected through a literature study and subsequently analyzed using descriptive qualitative analysis.

RESULTS AND DISCUSSION

A. Legal Regulation on the Governance of the Accountability of the Directorate General of Taxes for the Misuse of Digital Identity in the e-Faktur System

Digital identity refers to electronic data and information representing a person's personal data, ranging from the National Identity Number (Nomor Induk Kependudukan/NIK), fingerprints, or other official documents that may serve as proof of a person's identity. Digital identity naturally contains personal data that should receive legal protection from the state regarding the security and maintenance of such personal data. The general definition of personal data is provided in Article 1 point 1 of the Personal Data Protection Law, which states that: “Personal Data is data concerning an identified or identifiable individual, either separately or in combination with other information, whether directly or indirectly, through electronic or non-electronic systems.”(Firdaus, 2022) In the context of taxation, the digital identity formed from the elements of personal data referred to herein includes the National Identity Number (NIK), which has been designated as the same as the Taxpayer Identification Number (Nomor Pokok Wajib Pajak/NPWP) since 1 January 2024, the taxpayer's full name, telephone number, and financial data, each of which is classified under different categories of personal data.

The regulation concerning the protection of taxpayers' digital identities remains very limited under the KUP Law because it is explicitly regulated only in Article 34 paragraph (1), which states that: “Every official is prohibited from disclosing to any other party anything known to or informed to him or her by a Taxpayer in the course of his or her office or duties for the implementation of the provisions of laws and regulations.” This provision applies not only to tax officials but also to experts as stipulated in Article 34 paragraph (2) of the KUP Law, which provides that: “The prohibition referred to in paragraph (1) shall also apply to experts appointed by the Director General of Taxes to assist in the implementation of tax laws and regulations.” However, in practice, the provisions of these two paragraphs may be exempted, meaning that taxpayers' personal data may be disclosed to other parties under certain circumstances as stipulated in Article 34 paragraph (2a) of the KUP Law, which provides:

“Exempted from the provisions referred to in paragraph (1) and paragraph (2) are:

a. officials and experts acting as witnesses or expert witnesses in court proceedings; or

b. officials and/or experts designated by the Minister of Finance to provide information to officials of state institutions or government agencies authorized to conduct examinations in the field of state finance.”

This means that, apart from these two situations, taxpayers' personal data must remain confidential and its confidentiality must be maintained.(Alodia et al., 2024)

The term “official” in this context may refer to officials of the Directorate General of Taxes, the Directorate General of Customs and Excise, or regional government officials with authority in taxation. From this provision, it is understood that the prohibited subject is “every official,” meaning an individual vested with certain authority, who is prohibited from disclosing any taxpayer data. The prohibited act under this provision is the disclosure of taxpayers' personal data by an individual to another party. However, the Government has now officially implemented an electronic tax system, meaning that no “official” is directly involved because all processes are integrated into the system. Various electronic tax services are accommodated through DJP Online or Coretax, which provides major tax services, including the issuance of e-Faktur.

When a company first registers with the Directorate General of Taxes (DJP) to be confirmed as a Taxable Entrepreneur (Pengusaha Kena Pajak/PKP), the PKP is required to immediately apply for an Electronic Certificate, which will subsequently be used to access the e-Faktur application for issuing electronic tax invoices. The Electronic Certificate contains the NPWP as the primary digital identity. In addition to the NPWP, it also contains the taxpayer's name, public key, and the certificate validity period, all of which constitute the taxpayer's digital identity. If the Electronic Certificate is compromised, the digital identity contained therein is clearly at high risk of misuse.(Utami & Saleh, n.d.) Along with the development of electronic systems, digital identity breaches are no longer caused solely by officials unlawfully disclosing taxpayers' digital identities.

While it was appropriate for the mens rea to lie with tax officials when the tax system was still conducted manually, the shift to an electronic tax system has introduced risks associated with system failures. Although the use of electronic systems provides advantages such as user convenience, data integration, and the reduction of human error, it should also be recognized that electronic systems, particularly in Indonesia, still require considerable improvement, including with respect to data security. Electronically stored data is highly susceptible to breaches resulting from hacking or system failures. This is the aspect that has not yet been protected under the KUP Law, as the Law currently provides protection only against data breaches committed by tax officials without taking into account the risks arising from electronic tax services, including system failures or external hacking.

In response to this legal gap, the Government of Indonesia enacted the Personal Data Protection Law, which, in Article 1 point 2, defines personal data protection as follows: "Personal Data Protection is the entire series of efforts to protect Personal Data in the processing of Personal Data in order to guarantee the constitutional rights of Personal Data Subjects." Taxpayers fall within the scope of the definition of "Personal Data Subjects" protected under this Law. Within the taxation sector, the DJP may be classified as a "Personal Data Controller" by virtue of its authority. The definition of a Personal Data Controller is provided in Article 1 point 4 of the Personal Data Protection Law, which states that: "A Personal Data Controller is any individual, public body, or international organization acting individually or jointly in determining the purposes of and exercising control over the processing of personal data."(Devi, 2025) The DJP is authorized to process personal data submitted by taxpayers; therefore, Article 20 paragraph (2) letter (a) of the Personal Data Protection Law applies, which states that: "The legal basis for the processing of Personal Data as referred to in paragraph (1) includes: (a) the valid and explicit consent of the Personal Data Subject for one or more specific purposes communicated by the Personal Data Controller to the Personal Data Subject." Accordingly, any processing of personal data carried out by the DJP through electronic systems must obtain the taxpayer's consent.

The obligation to provide protection for the security of personal data is further clarified in Article 35 of the Personal Data Protection Law, which states that:

"A Personal Data Controller shall protect and ensure the security of the Personal Data it processes by:

a. preparing and implementing operational technical measures to protect Personal Data from processing that is contrary to the provisions of laws and regulations; and

b. determining the level of security of Personal Data by taking into account the nature and risks of the Personal Data that must be protected in the processing of Personal Data."

Furthermore, a Personal Data Controller is also obliged to prevent unauthorized access to personal data, including data breaches, as stipulated in Article 39 paragraph (1) of the Personal Data Protection Law, which states that: "A Personal Data Controller shall prevent Personal Data from being accessed without authorization."(Rusyda, 2025) Such unauthorized access also encompasses cybercrimes such as hacking and is not limited to individual misconduct as referred to in the KUP Law. The prevention of unauthorized access is carried out through the use of secure electronic security systems. It may therefore be understood that the Personal Data Protection Law provides not only administrative legal protection but comprehensive protection, and this serves as a concrete basis for evaluating the ability of Article 34 of the KUP Law to adapt to the provisions of the Personal Data Protection Law concerning the obligation to protect personal data and the parties responsible for ensuring its security.(Radithia & Inayati, 2021)

Article 34 of the KUP Law regulates the prohibition against officials disclosing taxpayers' personal data, including data categorized as digital identity, to any party unless permitted by law, such as for evidentiary purposes in court proceedings. The existence of such a prohibition gives rise to legal consequences if it is violated by the Directorate General of Taxes (DJP), meaning that the DJP must be held accountable for the violation it has committed. However, the KUP Law does not explicitly regulate the governance of the DJP's accountability with respect to the misuse of digital identities in the e-Faktur system, which may involve data misuse resulting from data breaches that do not involve DJP officials, such as system failures, phishing, or hacking. This constitutes a legal gap in the governance of the DJP's accountability.

Where the misuse of a digital identity is committed by a DJP official, the legal responsibility is clear. The responsibility referred to is criminal liability, as regulated in Article 41 of the KUP Law, which provides that:

(1) "An official who, through negligence, fails to fulfill the obligation to maintain confidentiality as referred to in Article 34 shall be subject to imprisonment for a maximum of 1 (one) year and a fine of not more than Rp25,000,000 (twenty-five million rupiah).

(2) An official who intentionally fails to fulfill such obligation, or any person who causes the official to fail to fulfill the obligation referred to in Article 34, shall be subject to imprisonment for a maximum of 2 (two) years and a fine of not more than Rp50,000,000 (fifty million rupiah).

(3) Prosecution of the criminal offenses referred to in paragraphs (1) and (2) shall only be initiated upon a complaint by the person whose confidentiality has been violated."

From this provision, it may be concluded that there is no obligation to compensate taxpayers whose personal data has been disclosed due to the negligence or intentional conduct of tax officials.(Cenvysta & Gunadi, 2024)

The provisions contained in Article 41 of the KUP Law only accommodate the misuse of digital identities resulting from the misconduct of DJP officials and do not regulate the accountability borne by the DJP as the personal data controller where the misuse arises from data breaches, phishing, or other similar cyberattacks within the e-

Faktur system. Therefore, it is appropriate that the provisions governing the DJP's accountability, which are currently contained only in Article 34 of the KUP Law, be reconstructed.

B. Reconstruction of the Governance of the Accountability of the Directorate General of Taxes in Providing Legal Certainty and Legal Protection against the Misuse of Digital Identity in the e-Faktur System

The regulation governing the accountability of the Directorate General of Taxes (DJP) in addressing the misuse of digital identity that is not caused by the misconduct of DJP officials is very limited, or even not regulated at all, under the KUP Law. This is reflected in Article 41 of the KUP Law, which provides that liability is imposed only on DJP officials who violate Article 34 of the KUP Law. In response to this legal gap, it is necessary to reconstruct the regulations concerning the governance of the DJP's accountability for the misuse of digital identity in the e-Faktur system. Such reconstruction is intended to amend, supplement, and/or complete existing legal provisions or establish regulations where none previously existed, so that they may adapt to changes and developments in society.

The dynamics of society are inherently dynamic, meaning that they continuously undergo change and development. Moreover, the advancement of technology has accelerated such changes, including developments in tax services, such as the process of issuing tax invoices, which can now be carried out digitally through the e-Faktur system. The development of society increases the complexity of legal issues that must be resolved through legislation. Therefore, in order for legislation to continue functioning as a regulatory instrument, legal norms must continually be adjusted through amendments and legal reform. Whereas previously the misuse of personal identity data was caused only by the negligence or intentional conduct of tax officials, new factors have emerged, such as data breaches resulting from phishing or hacking. Consequently, harmony between societal developments and statutory regulations is necessary. The reason for legal reconstruction is not merely that the existing law is no longer in line with societal developments but also that overlapping regulations will arise if legal norms are not promptly amended. This will ultimately affect the function of legal certainty within society.(Ganjar, 2025)

Law itself functions to provide protection to society, which, according to Mochtar Kusumaatmadja, is intended to achieve justice and social welfare for all Indonesian people.(Kusumaatmadja, 2006) Increasing the relevance of legislation to problems within society will also gradually improve public legal awareness. There are at least two criteria indicating why legislation should be reconstructed: (1) the existence of an urgent necessity and interest; and (2) the regulation concerned is a principal law affecting a particular field, such that failure to amend it will render implementing regulations irrelevant.(Mazli, 2021)

When assessed based on these two criteria, the reconstruction of the regulations governing the DJP's accountability for the misuse of digital identity within the e-Faktur service system satisfies both requirements. First, the KUP Law currently contains no provisions governing taxation within electronic or digital systems, resulting in uncertainty regarding the DJP's accountability when legal issues arise in digital systems. Therefore, this constitutes an urgent necessity and interest because, without immediate regulation, no legislation will provide legal protection and legal certainty for taxpayers. Second, the KUP Law is the principal legislation in the field of taxation and therefore affects other legislation of the same hierarchical level as well as subordinate regulations. As an Act, it is capable of establishing criminal sanctions as a form of legal accountability. Accordingly, it is appropriate that the KUP Law be reconstructed so that provisions concerning criminal sanctions may be incorporated.

The reconstruction of the KUP Law is also important because digital taxation systems have not yet been regulated therein. Consequently, when misuse or data breaches involving digital identities occur, no legislation in the field of taxation provides legal protection and legal certainty for taxpayers. The causes of personal data breaches may be classified into three factors: (1) human error, which generally occurs when tax services are provided manually but may also occur in digital services, such as entering an incorrect password or committing other errors that intentionally or unintentionally enable unauthorized access to personal data; (2) malware attacks, which may occur due to user negligence in unintentionally installing malicious software such as spyware into computer systems, allowing the collection of users' personal data and its covert transmission to third parties over an extended period, particularly given that Indonesia's electronic security systems remain relatively weak; and (3) social engineering, which involves psychological manipulation by impersonating a trusted party in order to gain access to information systems containing various personal data, ranging from names to taxpayers' NPWPs, for subsequent misuse.(Soleh & Tjenren, 2025)

The proposed reconstruction may be carried out by adopting provisions from other legislation governing the protection of personal data, whether in conventional or electronic forms. One provision that may be adopted in reconstructing the DJP's accountability framework is Article 47 of the Personal Data Protection Law, which provides that: “A Personal Data Controller shall be responsible for the processing of Personal Data and shall demonstrate accountability in fulfilling its obligations to implement the principles of Personal Data Protection.” This provision clearly regulates the responsibility of a Personal Data Controller to safeguard the confidentiality of personal data, the violation of which gives rise to legal consequences in the form of administrative sanctions, as affirmed in Article 57 paragraph (1) of the Personal Data Protection Law. The administrative sanctions referred to are further specified in Article 57 paragraph (2) of the Personal Data Protection Law, which states:

“The administrative sanctions referred to in paragraph (1) consist of:
a. a written warning;
b. temporary suspension of personal data processing activities;
c. deletion or destruction of personal data; and/or
d. an administrative fine.”

The administrative fine that may be imposed is a maximum of 2% (two percent) of the annual revenue or annual income of the Personal Data Controller.(Mahendra et al., 2025) This form of reconstruction is directed at the provisions of Article 34 of the KUP Law, which currently regulate only the prohibition against officials disclosing personal data without taking into account the impact of technological developments.

CONCLUSION

Indonesia does not yet have legal regulations governing the accountability of the Directorate General of Taxes for the misuse of digital identity in the e-Faktur system. The existing regulation is limited to Article 34 of the KUP Law, which prohibits the disclosure of taxpayers' personal data by officials, with the corresponding form of liability being imprisonment and fines as stipulated in Article 41 of the KUP Law. This demonstrates the existence of a legal gap, considering that the disclosure of taxpayers' personal data used to issue e-Faktur may now occur not only through DJP officials but also due to other factors causing data breaches, such as phishing or hacking. Therefore, it is necessary to reconstruct the regulations governing the DJP's accountability by adopting the provisions contained in Article 47 of the Personal Data Protection Law, which designates the DJP as a Personal Data Controller and requires it to be accountable in the event of a data breach. The form of accountability referred to consists of the implementation of administrative sanctions and may also include criminal sanctions.

REFERENCES

Alodia, I., Widjiatuti, A., & Xaverius, F. (2024). Optimalisasi Pelindungan Hukum Data Wajib Pajak Pada Penerapan Sistem Automatic Exchange Of Information (AEoI). *Jurnal Hukum Lex Generalis*, *5*(12).

Ardin, G. (2022). Estimasi Dampak Fiskal Penggunaan NIK Sebagai NPWP: Sebuah Studi Empiris. *Jurnal Pajak Dan Keuangan Negara (PKN)*, *4*(1), 33–42.

Cenvysta, M., & Gunadi, A. (2024). Konsep Tanggung Jawab Negara Terhadap Kewajiban Melindungi Data Pribadi Masyarakat Di Indonesia (Studi Kasus Kebocoran Data NPWP Masyarakat Indonesia). *Rewang Rancang: Jurnal Hukum Lex Generalis*, *5*(12), 1–14.

Devi, I. G. A. P. G. (2025). Analisis UU ITE Dan Perlindungan Data Pribadi: Implikasi Tanggung Jawab Pidana Dalam Kasus Doxing Pada Pemilu 2024. *Referendum: Jurnal Hukum Perdata Dan Pidana*, *2*(2), 67–77.

Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *4*(2), 23–31.

Ganjar, S. D. (2025). Urgensi Pembaruan Hukum Pidana Dalam Menanggulangi Kejahatan Siber: Tinjauan Kritis Terhadap Kesesuaian KUHP Nasional Dan Perubahan UU ITE. *Locus Journal of Academic Literature Review*, *4*(3), 197–208.

Indriastuti, Desy, Jaya, I., Tridianto, A., Taberima, V. A., Rompas, J. T., Hutauruk, A., & Simanjuntak, R. L. (2025). Implikasi Hukum Atas Penyalahgunaan E-Faktur Oleh Wajib Pajak Dan Badan Usaha: Aspek Pidana, Gugatan Perdata, Dan Perlindungan Hukum Bagi Pihak Ketiga Yang Dirugikan. *Arus Jurnal Sosial Dan Humaniora (AJSH)*, *5*(2), 3104–13.

Kusumaatmadja, M. (2006). *Konsep-Konsep Hukum Dalam Pembangunan* (Alumni).

Mahendra, B. T., Hafrida, & Liyus, H. (2025). Kebijakan Hukum Pidana Terhadap Penyebaran Data Pribadi (Doxing) Jurnalis Dalam Rangka Perlindungan Data Pribadi Di Indonesia. *Rio Law Jurnal*, *1*(2), 643–50.

Mazli, A. (2021). Urgensi Pembaharuan Undang-Undang Perlindungan Konsumen Indonesia Di Era E-Commerce. *Lex Renaissan*, *2*(6), 298–312.

Melani, R. A., & Doloksaribu, E. I. (2024). Tinjauan Yuridis Integrasi NIK Menjadi NPWP. *Jurnal Paradigma Hukum Pembangunan*, *9*(1), 1–18.

Nurmala, S. A., & Wiraguna, S. A. (2026). Analisis Yuridis Tanggung Jawab Direktorat Jenderal Pajak (DJP) Terhadap Kebocoran Data Nomor Pokok Wajib Pajak (NPWP) Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Kajian Ilmiah*, *26*(1), 2026.

Pamungkas, T. J., & Hariri, A. (2022). Tanggung Jawab Negara Dalam Pemenuhan Jaminan Sosial Perspektif Welfare State. *Media of Law and Sharia*, *3*(4), 270–83.

Primayudhana, M. A. (2025). Implementasi Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Dalam Digitalisasi Perpajakan Di Indonesia. *Mahalini: Journal of Business Law*, *2*(2).

Radithia, & Inayati. (2021). Kesiapan Direktorat Jenderal Pajak (DJP) Dalam Pemungutan Pajak Digital Berdasarkan Faktor Individual. *Syntax Literate: Jurnal Ilmiah Indonesia*, *6*(12), 6296–6304.

Rusyda, N. K. (2025). Perlindungan Hukum Terhadap Subjek Data Kebocoran Data Oleh Badan Publik Menurut UU Nomor 27 Tahun 2022. *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan*, *22*(3), 247–62.

Siregar, R. W., Sinaga, N. A., & Gaol, S. L. (2024). Kajian Hukum Atas Tindak Pidana Pemalsuan Faktur Pajak Yang Telah Memperoleh Pengampunan Pajak. *Jurnal Hukum Sehasen*, 2567–576.

Soleh, M., & Tjenren, Z. (2025). Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital. *Jurnal Kajian Pemerintah: Journal of Government, Social and Politics*, *11*(1), 1–10.

Sugono, D. (2018). *Kamus Besar Bahasa Indonesia*. Kamus Pusat Bahasa Depdiknas.

Tan, D. (2021). Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *8*(8), 2463–78.

Utami, R. D. C., & Abd, R. S. (2024). Kajian Yuridis Penegakan Hukum Pajak Terhadap Pembuat Dan Pengguna Faktur Pajak Tidak Berdasarkan Transaksi Sebenarnya (TBTS). *Innovative: Journal Of Social Science Research*, *4*(1), 2863–74.

Utami, & Saleh. (n.d.). *Kajian Yuridis Penegakan Hukum Pajak Terhadap Pembuat Dan Pengguna Faktur Pajak Tidak Berdasarkan Transaksi Sebenarnya (TBTS)*.

Wange, W., & Katili, A. Y. (2024). Tantangan Dan Peluang Dalam Implementasi Sistem Perpajakan Berbasis Teknologi Informasi Di Indonesia. *Jurnal Administrasi, Manajemen Sumber Daya Manusia, Dan Ilmu Sosial (JAEIS)*, *3*(3), 166–75.

Publish by **Radja Publika**