

Protection of taxpayer personal data in tax administration: a review

Loso Judijanto

IPOSS Jakarta

Indonesia Palm Oil Strategic Studies, Indonesia

Article Info

Article history:

Received: Sept 06, 2024

Revised: Sept 17, 2024

Accepted: Sept 23, 2024

Keywords:

Data Security;
Personal Data Protection;
Privacy;
Tax Administration;
Taxpayer Trust.

ABSTRACT

The protection of personal data in tax administration is a critical issue in the digital age. Tax authorities collect and process vast amounts of personal data from taxpayers, raising concerns about privacy and data security. This research explores the importance of safeguarding taxpayer privacy in tax administration. It examines the legal and regulatory frameworks governing personal data protection in the tax context, emphasizing the need for robust data security measures and transparent data handling practices. The study also discusses the potential consequences of data breaches and privacy violations, highlighting the importance of building trust between taxpayers and tax authorities. The research concludes by emphasizing the need for ongoing efforts to strengthen personal data protection in tax administration to ensure taxpayer privacy and maintain public confidence in the tax system.

This is an open access article under the [CC BY-NC](#) license.



Corresponding Author:

Loso Judijanto

IPOSS Jakarta, Indonesia Palm Oil Strategic Studies, Indonesia

Gedung Sahid Sudirman Lantai 16 Jalan Jendral Sudirman Kav. Jakarta Pusat, Indonesia, 10220.

Email: losojudiantobumn@gmail.com

1. INTRODUCTION

The protection of personal data in tax administration is increasingly crucial in today's digital age. As information technology advances, tax agencies have greater access to taxpayers' personal data. This also raises concerns about the privacy and security of the personal data. A comprehensive approach to personal data protection is not only important to safeguard individual privacy, but also to maintain public trust in tax agencies. In the context of tax administration, taxpayers' personal data is a valuable asset for tax agencies in conducting tax collection, monitoring, and investigation (Bassey, Mulligan and Ojo, 2022).

Data security and privacy are major concerns for both tax authorities and taxpayers. According to Schwartz and Solove (2011), personal data includes any information that can be used to identify a person either directly or indirectly (Batara Randa and Haryanto, 2021). In the context of taxation, taxpayer personal data includes information such as name, address, tax identification number, income details, and other financial data. The protection of taxpayer personal data has become increasingly crucial along with the implementation of an information technology-based taxation system. Tax authorities in various countries have adopted electronic tax administration systems to improve the efficiency and effectiveness of tax collection. However, the use of information technology also carries the risk of leakage or misuse of taxpayer data. According to the OECD report (2020), the incidence of data breaches in the taxation sector has increased significantly in recent years (Amalia, 2020). This shows the importance of strengthening the protection of taxpayer personal data.

On the other hand, tax authorities need access to sufficient taxpayer data to carry out their functions in collecting taxes and preventing tax evasion. There is a potential conflict between the need for data transparency for tax purposes and the privacy rights of taxpayers. According to Cockfield (2010), a balance is needed between the government's interest in accessing taxpayer information and the protection of individual privacy (Rolamdo and Widiastuti, 2021). Personal data protection regulations must be able to accommodate both interests. The development of big data technology and artificial intelligence also brings new challenges in taxpayer data protection. Tax authorities now have the ability to collect and analyze taxpayer data on a large scale. According to Houser and Sanders (2017), the use of big data analytics in tax administration has the potential to violate taxpayer privacy if not properly regulated (Pane, 2017). A comprehensive legal framework is needed to regulate the use of such technology while protecting the rights of taxpayers.

Various countries have implemented personal data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union. However, the application of this regulation in the context of taxation still faces various challenges. According to Debelva and Mosquera (2017), there is a potential conflict between data protection obligations under the GDPR and tax information exchange obligations between countries (Melani and Dolok, 2024). Harmonization between data protection regulations and tax law is an important issue that needs to be studied further. In Indonesia, the protection of taxpayer personal data is regulated in various laws and regulations such as the Law on General Provisions and Tax Procedures (KUP) and the Law on Personal Data Protection. However, the implementation of taxpayer data protection still faces various obstacles. According to Rosdiana and Irianto (2014), there are still weaknesses in the institutional aspects and information technology infrastructure that support the protection of taxpayer data in Indonesia (Septia and Supriyo, 2023). It is necessary to strengthen the regulation and capacity of tax authorities in managing taxpayer data.

Previous research has examined various aspects of taxpayer personal data protection. For example, Zalnieriute et al. (2017) analyzed the data protection implications of automatic tax information exchange between countries (Sudjana, 2022). Meanwhile, Blank (2011) discusses the trade-off between tax data transparency and taxpayer privacy. However, there is still a need for a comprehensive study that integrates these various perspectives, especially in the context of recent technological developments.

2. METHOD

Based on this background, this article aims to review the current issues in taxpayer personal data protection. Specifically, this article will examine the legal and regulatory framework for taxpayer data protection, challenges in implementing data protection in the big data era, the balance between transparency and privacy in tax administration, and policy recommendations for strengthening taxpayer data protection. The results of the study are expected to contribute to the development of data protection policies in tax administration. This research uses a qualitative method with a literature review approach to explore issues related to taxpayer personal data protection. The data sources used include journal articles, research reports, regulations, and relevant policy documents. The analysis is done thematically to identify key issues and develop a synthesis of various perspectives. Through a comprehensive literature review, this research is expected to provide a holistic picture of taxpayer data protection and identify future research agendas (Afiyanti, 2014; Rosid, 2016; Kalpokaite and Radivojevic, 2021; Afandi et al., 2022; Tenny, Brannan and Brannan, 2022)..

3. RESULTS AND DISCUSSION

Definition of Taxpayer Personal Data

Taxpayer personal data refers to information that can directly or indirectly identify an individual and is related to tax obligations. This may include information such as name, address, identity number, bank account number, and other tax information. This definition is in line with Law No. 11/2008 on Electronic Information and Transactions, which regulates the protection of personal data in Indonesia. According to the Act, personal data is information about an individual who can be identified, either directly or indirectly, through identification such as name, identification number, location of certain electronic or physical data, or one or more specific factors that constitute the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Taxpayer personal data is any information that directly or indirectly identifies or can identify a tax subject. This includes information such as tax identification numbers, financial information, and tax payment history (Nasution, 2020).

The Importance of Personal Data Protection in Tax Administration

Personal data protection in tax administration has several important aspects to consider. First, personal data protection is important to maintain the security of tax information. Sensitive information such as financial data and personal identity can be targeted by illegal parties for fraud or other crimes. By securing taxpayers' personal data, the risk of misuse and identity theft can be minimized (Setyawan, 2023). Personal data protection in tax administration is important to prevent unauthorized access to sensitive information that could harm tax subjects. Irresponsible parties can exploit information by committing criminal acts such as tax evasion or identity fraud that can harm the state and taxpayers themselves (Kurniawan, 2018).

Personal data protection is also important to maintain taxpayer privacy. As individuals or entities that pay taxes, taxpayers have the right to maintain the confidentiality of their respective personal information. In the context of transparent tax administration, it is important for tax authorities to ensure that taxpayers' personal information is not misused or accessed without proper authorization. Personal data protection in tax administration is an important aspect of maintaining taxpayers' privacy and trust in tax institutions. Taxpayers must feel comfortable and trust that personal information will be kept confidential by tax agencies. This is crucial in maintaining harmonious relations between tax authorities and taxpayers and to encourage better tax compliance (Siregar, 2021).

In order to maintain the security and privacy of taxpayers' personal data, protective measures such as data encryption, the use of information security technology, and compliance with data protection regulations need to be strictly implemented in tax administration. Data encryption is an effective technique in providing protection to sensitive information against illegal access as it converts plain text into encrypted text that can only be opened by a party with the appropriate encryption key. The use of information security technologies, such as firewalls and antivirus, is also important to prevent cyber attacks and data leakage (Rulandari et al., 2022). In addition, tax agencies need to ensure compliance with data protection regulations such as Law Number 11 of 2020 on Electronic Information and Transaction Systems (ITE Law) and Law Number 27 of 2022 on Personal Data Protection (PDP Law). Compliance with these regulations will assist tax agencies in establishing adequate systems and procedures to protect taxpayers' personal data and ensure that taxpayers' privacy rights are respected (Matabean and Juwono, 2021; Rulandari et al., 2022).

By paying attention to these aspects, tax agencies can ensure that the protection of taxpayers' personal data is properly integrated in tax administration. This will help maintain information security, safeguard taxpayer privacy, and strengthen public trust in tax agencies. As a result, efficient and effective tax administration can be realized, which in turn will support economic growth and public welfare (Matabean and Juwono, 2021; Rulandari et al., 2022).

Personal Data Protection in Tax Administration

Personal data protection is a major focus in today's digital era, especially in the context of tax administration. Tax administration involves collecting, processing, and storing taxpayers' personal data for tax purposes. However, with the advancement of technology and increasing cyber security threats, the protection of personal data has become increasingly important (Matabean and Juwono, 2021). In tax administration, taxpayer personal data includes personal information such as name, address, tax identification number, and other financial information. Loss, leakage, or misuse of this data can have serious repercussions for both individuals and the government (Setyawan, 2023).

Related Regulations and Policies

In the context of personal data protection in tax administration, two aspects of regulation and policy are particularly relevant: personal data protection regulation and privacy policy in tax administration. These two aspects play a crucial role in maintaining the security and privacy of taxpayers' personal data and ensuring tax agencies' compliance with applicable standards and regulations.

Personal Data Protection Regulation

Personal data protection regulations are the legal basis that regulates the collection, processing, storage, and use of personal data by tax agencies. In Indonesia, Law Number 11 of 2020 on Electronic Information and Transaction Systems (ITE Law) and Law Number 27 of 2022 on Personal Data Protection (PDP Law) are the main regulations governing personal data protection. The ITE Law and PDP Law regulate individuals' rights to data privacy and provide a framework for the protection of personal data from cybersecurity threats and misuse. More technically, there is also Government Regulation (PP) No. 71/2019 on the Implementation of the ITE Law that further regulates the protection of personal data. This PP provides technical provisions on personal data protection, such as information security standards, data manager obligations, and data breach reporting procedures.

The implementation of the Personal Data Protection Law is still faced with several challenges, especially in the context of tax administration. One of the main challenges is how the government can integrate the principles of personal data protection in the tax administration system without hampering the efficiency and effectiveness of the taxation process (Sukmawati, 2019). The implementation of this regulation in the context of tax administration requires concrete steps from tax agencies to ensure that every step of collecting, processing, and storing taxpayers' personal data is carried out in accordance with established data protection standards. This includes the establishment of internal policies, employee training, the use of information security technology, and regular audits to ensure compliance with regulations (Setyawan, 2023).

Privacy Policy in Tax Administration

Privacy policies in tax administration govern how tax agencies interact with taxpayers' personal data and maintain the confidentiality of that information. This policy includes steps taken by tax agencies to ensure that taxpayers' personal data is not misused or accessed by unauthorized parties (Wohrer, 2018). Within the framework of the privacy policy, tax agencies need to have clear policies regarding the utilization and disclosure of taxpayer personal data. This includes regulating access to data, limiting the use of data only for legitimate tax purposes, and mechanisms for deleting data that is no longer needed (Wohrer, 2018).

In addition, privacy policies also involve efforts to increase employees' awareness and understanding of the importance of data privacy. Regular training on privacy policies and proper procedures in handling taxpayers' personal data is key to preventing privacy breaches and reducing the risk of data leaks (Setyawan, 2023). With the existence of personal data protection regulations and strong privacy policies in tax administration, it is expected that tax agencies can properly maintain the security and privacy of taxpayers' personal data. This not only protects individuals' rights to privacy but also ensures the integrity and public trust in the tax system as a whole. The importance of integration between tax regulations and personal data protection policies to ensure that taxpayers' personal data is not misused or illegally accessed by unauthorized persons (Pratama, 2020).

Taxpayer Personal Data Collection and Storage

The collection and storage of taxpayer personal data is an integral part of effective tax administration. Such data forms the basis for the government to set and manage tax policies and ensure tax compliance. But this process also requires careful consideration of information privacy and security.

Data Collection Process

The collection of taxpayer personal data can be done through various means, including tax forms, financial statements, and information from third parties such as financial institutions or employers. This process must observe the principles of privacy and legal compliance. It is important to apply the principles of fairness, transparency and autonomy in data collection. This ensures that taxpayers provide information voluntarily and understand the purpose of using the data (Sari and Wibowo, 2019).

Principles of Safe Storage

Once the data is collected, the next step is secure storage. The following principles help maintain the confidentiality and integrity of taxpayers' personal data: Data Encryption, Data should be stored in an encrypted format to prevent unauthorized access. Strong encryption methods such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) can be used to protect sensitive information (Pratama and Kurniawan, 2020). Access Management, Only authorized staff may access taxpayer personal data. A strict access management system and double authentication are required

to ensure that only authorized parties can view or manipulate the information (Aditya and Cahyani, 2021): Secure Cloud-Based Storage, Cloud-based storage options are becoming popular due to their flexibility and scalability. However, it is important to choose a service provider that prioritizes security and compliance, and implements strict access controls (Darmawan and Wijaya, 2018): Activity Monitoring, Monitoring systems should be implemented to detect suspicious activity or potential security breaches. Proactive measures can prevent further losses in the case of data leakage (Utama and Widiantara, 2017). Secure storage is a crucial aspect in the protection of taxpayer personal data. By applying these principles, the government can ensure that sensitive information is well protected and taxpayer trust is maintained.

Access and Use of Personal Data

In this increasingly digital age, personal data has become an extremely valuable asset. But with great value comes great responsibility to protect the security and privacy of that data. Two important aspects that must be considered are restricting access to data and using data only for legitimate purposes.

Restriction of Access to Data

Restriction of access to data is a fundamental principle in personal data protection. It involves controlling who has the right of access to one's personal data. In the context of personal data administration. Use of Authorization System: Appropriate authorization systems should be implemented to ensure that only authorized parties have access to personal data. This includes granting access permissions based on job responsibilities and business needs. The implementation of a strict authorization system can reduce the risk of data security breaches and misuse of access (Nurliyana, 2019).

Using encryption technology to protect personal data as it moves between systems or is stored in a database. Encryption can help prevent unauthorized access even if the data is successfully captured by irresponsible parties. Data encryption is one of the effective methods in protecting the security of personal data from cyber attacks (Cahyani and Sari, 2020).

Use of Data for Lawful Purposes Only

In addition to access restrictions, it is also important to ensure that personal data is only used for legal purposes and in accordance with the needs or applicable regulations. Establishment of Data Use Policy: Organizations must have a clear policy regarding the use of personal data including the limitations on its use. This policy should be consistently applied by all personnel who have access to the data (Dharma, 2018).

Monitoring of Data Use: The organization should have a monitoring mechanism to check whether the use of personal data is in accordance with the established policy. This can be done through periodic internal audits. This can help prevent data misuse and strengthen compliance with data protection regulations (Utami and Widyawati, 2021). In managing personal data, restricting access and using data only for legitimate purposes are crucial principles. By implementing appropriate measures, organizations can more effectively maintain the security and privacy of taxpayers' personal data.

Effective Personal Data Protection Measures

Personal data protection is very crucial, especially in the context of tax administration. Taxpayers submit personal information to the authorities for tax purposes. Effective personal data protection measures are therefore necessary to ensure that such sensitive information is not misused or stolen by unauthorized parties.

Tax Officer Certification and Training

Tax officers have access to taxpayers' personal information in carrying out their duties. Tax officers must be equipped with the right understanding and expertise in managing and protecting this personal data. Ongoing training and certification programs related to personal data protection can help tax officers to understand the importance of data privacy and best practices in managing sensitive information. Thus, they will be more vigilant and careful in securing and protecting taxpayers' personal data from potential security threats (Fitriyani, 2019).

Use of Latest Information Security Technology

The use of the latest information security technologies is another important step in improving the protection of personal data in tax administration. These technologies include various systems and software specifically designed to secure and protect the integrity of personal data. Technologies such as data encryption, firewalls, and cyber threat detection can help in preventing unauthorized access to sensitive information (Susanto, 2020). In addition, the use of blockchain technology has also been proposed as a solution to increase the level of security and transparency in tax data management (Nugroho, 2018).

By implementing these latest information security technologies, tax administrations can ensure that taxpayers' personal data remains secure and protected from potential security threats. Personal data protection in tax administration is a fundamental responsibility that cannot be ignored. By taking measures such as certification and training of tax officers and the use of the latest information security technologies, the security and integrity of taxpayers' personal data can be enhanced. These efforts are essential to ensure taxpayer trust and compliance with the tax system, and to protect the privacy rights of taxpayer data.

Challenges and Implications

Personal data protection is already a major issue faced by various institutions, including tax agencies. As the use of information technology in tax administration increases, the challenges in maintaining the security and privacy of taxpayers' personal data also become more complex. It is important to understand the challenges faced in the protection of taxpayers' personal data as well as the implications arising from breaches of such data protection.

The main challenges faced include increasingly sophisticated cybersecurity threats, regulatory limitations in addressing new technological developments, and a lack of awareness of the importance of personal data protection among taxpayers and tax agencies themselves. In addition, violations of personal data protection can have far-reaching impacts, including legal and financial penalties for tax agencies, as well as loss of reputation and public trust.

By understanding these challenges, tax agencies can take proactive steps to improve data security and ensure compliance with applicable personal data protection regulations. In addition, awareness of the implications of personal data protection breaches can serve as an impetus for tax agencies to improve systems and procedures to effectively protect taxpayers' personal data.

Challenges in Managing Taxpayer Personal Data

Taxpayer personal data is a very valuable asset in tax administration. However, managing such personal data is not easy and is often faced with various challenges. Two of the main challenges faced are data security which is vulnerable to cyber-attacks and concerns related to constant regulatory changes.

Data Security Vulnerable to Cyber Attacks

Taxpayers' personal data, such as tax identification numbers, financial information and contact data, are prime targets for cyber criminals. Cyber-attacks on taxpayer personal data can result in substantial financial losses and reputational damage to the tax agencies responsible for managing such data. Cyber-attacks on taxpayers' personal data have seen a marked increase in recent years. This shows the need for proactive measures to improve data security, including the implementation of encryption technology, strong firewalls, and active monitoring of suspicious activity in the system (Pramudya, 2019).

Regulatory Compliance

Regulations related to personal data protection and tax administration change frequently, both in terms of substance and technical requirements. The main challenge for parties managing taxpayer personal data is to remain compliant with these changing regulations without disrupting smooth operations. The importance of compatibility and adaptability in dealing with regulatory changes related to the protection of taxpayer personal data. Industry players and regulators must work together to ensure that new policies are implemented effectively and without creating excessive obstacles for taxpayers (Susanto and Hartono, 2020).

Managing taxpayer personal data is a big responsibility that cannot be taken lightly. Data security challenges and changing regulations are two key aspects that must be addressed in a proactive and organized manner. By understanding the risks involved and implementing appropriate

measures, the parties involved can ensure that taxpayers' personal data remains safe and secure in tax administration.

Implications of Personal Data Protection Breaches

Personal data protection is increasingly critical in today's digital age. Institutions, including tax agencies, are responsible for the personal data they manage. A personal data protection breach can have significant legal, financial and reputational repercussions. This chapter will explore the implications of a personal data protection breach, particularly in the context of tax agencies.

Legal and Financial Impacts for Tax Agencies

Violations of personal data protection can lead to serious legal consequences for tax agencies. Personal data protection laws, such as Law No. 11 of 2020 on Electronic Information Systems and Transactions (ITE Law) and Law No. 27 of 2022 on Personal Data Protection in Indonesia provide a clear framework on personal data protection and sanctions for violators. Violations of these laws can result in significant fines for tax agencies responsible for leaked or misused data. In addition, tax agencies that violate personal data protection may also face lawsuits from individuals whose personal data was affected by the breach. These lawsuits can impose enormous costs in terms of litigation, settlements, and compensation to the affected individuals. Personal data breaches by tax agencies can result in significant financial losses. The costs incurred by tax agencies to address the impact of personal data breaches include investigation costs, data recovery, and fines to be paid (Siswanto and Tampubolon, 2019).

Loss of Reputation and Public Trust

Personal data protection breaches can also damage the reputation of tax agencies and public trust. When taxpayers' personal data is leaked or misused, it can create great distrust of the tax agency in charge. The public becomes concerned about data privacy and security, which can lead to a decrease in trust and support for the tax policies implemented. The importance of reputation in maintaining public trust in tax agencies. A breach of personal data by tax agencies can lead to a significant decline in the public's perception of the integrity and competence of the tax. Damaged trust can have a negative impact on tax revenue, policy enforcement, and public support for tax programs (Prasetyo and Wahyudi, 2021). Personal data protection breaches by tax agencies have serious consequences including significant legal and financial repercussions as well as loss of reputation and public trust. It is therefore important for tax agencies to take proactive steps to protect taxpayers' personal data and ensure compliance with personal data protection laws.

4. CONCLUSION

This paper has taken an in-depth look at the protection of taxpayers' personal data in tax administration, an increasingly important issue in today's digital age. With the advancement of information technology, tax agencies have greater access to taxpayers' personal data, but this also poses the risk of misuse and invasion of privacy. Therefore, the protection of taxpayers' personal data is a necessity that cannot be ignored. The importance of personal data protection in tax administration relates not only to information security, but also to public trust in tax agencies. When taxpayers feel confident that personal data will be properly protected, they will be more trusting and cooperative in fulfilling tax obligations. Conversely, privacy violations can undermine that trust and hinder the effectiveness of tax administration. In an effort to protect taxpayers' personal data, various measures have been taken including the implementation of personal data protection regulations, the development of strict privacy policies, and the use of the latest information security technologies. However, challenges remain, especially in the face of evolving cybersecurity threats and dynamic regulatory changes. Tax agencies need to continuously update systems and procedures to remain relevant and effective in protecting taxpayers' personal data. Training and certification of tax officers is also important to ensure they have adequate knowledge and skills in managing sensitive data. In addition, collaboration between tax agencies, information technology experts, and other stakeholders is needed to develop innovative solutions to the increasingly complex challenges of personal data protection.

Recommendations for Future Studies Further research is needed to explore various aspects of personal data protection in tax administration. Some areas that can be the focus of future research include: Evaluation of the effectiveness of the implementation of personal data protection regulations

in tax administration: This research can identify the strengths and weaknesses of the current regulatory implementation, as well as provide recommendations for improvement. Comparative study on taxpayer personal data protection in various countries: This research can provide insights into best practices that can be adopted and adapted to the Indonesian context. Analysis of the impact of new technologies, such as artificial intelligence (AI) and blockchain, on the protection of taxpayers' personal data: This research can help anticipate the challenges and opportunities that arise with technological developments. Development of a comprehensive and adaptive personal data protection model: This model should be able to address evolving cybersecurity challenges and dynamic regulatory changes. Study on taxpayers' perceptions of personal data protection: This research can provide valuable input for tax agencies in improving tax policies and practices. By conducting further research in this area, it can be expected that the protection of taxpayers' personal data remains a top priority in tax administration so as to create a safe, fair and efficient tax system.

REFERENCES

- Aditya, B. and Cahyani, D.A. (2021) 'Manajemen Akses dalam Sistem Informasi Pajak: Studi Kasus di Indonesia', *Jurnal Teknologi Informasi dan Komunikasi*, 15(2), pp. 112–125.
- Afandi, A. et al. (2022) *Metodologi Pengabdian Masyarakat*. 1st edn, Metodologi Pengabdian Masyarakat. 1st edn. Edited by Suwendi, A. Basir, and J. Wahyudi. Jakarta: Ditjen Pendidikan Islam Kementerian Agama RI. Available at: <https://repository.uinjkt.ac.id/dspace/bitstream/123456789/71356/1/Buku.pdf>.
- Afiyanti, Y. (2014) 'Penggunaan Literatur dalam Penelitian Kualitatif', *Jurnal Keperawatan Indonesia*, 9(1), pp. 2003–2006. Available at: <https://doi.org/10.7454/jki.v9i1.157>.
- Amalia, H. (2020) *Perlindungan Hukum terhadap Wajib Pajak di Indonesia Pasca Penerapan Undang-Undang Nomor 9 Tahun 2017 melalui Pendekatan Hak Asasi Manusia*. Universitas Gadjah Mada Yogyakarta. Available at: <https://etd.repository.ugm.ac.id/penelitian/detail/194341>.
- Bassey, E., Mulligan, E. and Ojo, A. (2022) 'A conceptual framework for digital tax administration - A systematic review', *Government Information Quarterly*, 39(4), p. 101754. Available at: <https://doi.org/10.1016/j.giq.2022.101754>.
- Batara Randa, I.D. and Haryanto, I. (2021) 'Perlindungan Hukum atas Data Wajib Pajak dalam Sistem Automatic Exchange of Information (AEol): Studi Perbandingan Indonesia dan Uni Eropa', *Legal Standing: Jurnal Ilmu Hukum*, 5(1), p. 25. Available at: <https://doi.org/10.24269/ls.v5i1.3563>.
- Cahyani, R. and Sari, R. (2020) 'Implementasi Enkripsi Data dalam Sistem Informasi Akademik Berbasis Web untuk Meningkatkan Keamanan Informasi', *Jurnal Sistem Informasi Dan Teknologi*, 4(2), pp. 59–66.
- Darmawan, F.R. and Wijaya, A. (2018) 'Keamanan Penyimpanan Berbasis Cloud dalam Konteks Perpajakan', *Jurnal Sistem Informasi Bisnis*, 6(3), pp. 201–214.
- Dharma, I.G.A.G.N. (2018) 'Manajemen Data Pribadi Dalam Penyelenggaraan Administrasi Kependudukan Di Desa', *Jurnal Kajian Informasi & Perpustakaan*, 6(1), pp. 89–98.
- Fitriyani, R. (2019) 'Pelatihan dan Sertifikasi Pegawai dalam Menyikapi Perkembangan Teknologi Informasi pada Instansi Pajak', *Jurnal Administrasi Pajak*, 3(1), pp. 25–36.
- Kalpokaite, N. and Radivojevic, I. (2021) 'Adapting Practices from Qualitative Research to Tell a Compelling Story: A Practical Framework for Conducting a Literature Review', *The Qualitative Report*, 26(5), pp. 1546–1566. Available at: <https://doi.org/https://doi.org/10.46743/2160-3715/2021.4749>.
- Kalyon, A. (2022) 'The Privacy Right of Legal Person Taxpayer', *Maliye Çalışmaları Dergisi / Journal of Public Finance Studies*, 0(67). Available at: <https://doi.org/10.26650/mcd2022-1074312>.
- Kurniawan, B. (2018) 'Keamanan Data Pribadi Wajib Pajak dalam Administrasi Pajak', *Jurnal Keuangan dan Pajak*, 12(3), pp. 78–89.
- Matabean, R. and Juwono, V. (2021) 'Implementation of Data Collection Policy and Tax Information on Directorate General of Taxes', *Jurnal Borneo Administrator*, 17(3), pp. 365–378. Available at: <https://doi.org/10.24258/jba.v17i3.872>.
- Melani, R.A. and Dolok, E.I. (2024) 'Tinjauan Yuridis Integrasi NIK Menjadi NPWP', *Jurnal Paradigma Hukum Pembangunan*, 9(1(Februari)). Available at:

- <https://ejournal.atmajaya.ac.id/index.php/paradigma/article/download/5218/2437/21137>.
- Nasution, A. (2020) 'Perlindungan Data Pribadi Wajib Pajak dalam Administrasi Pajak', *Jurnal Administrasi Pajak*, 8(2), pp. 45–56.
- Nugroho, A.B. (2018) 'Penerapan Teknologi Blockchain dalam Pemungutan Pajak', *Jurnal Ekonomi Pajak*, 7(2), pp. 45–56.
- Nurliyana, I.G.A.A. (2019) 'Penerapan Sistem Otorisasi Berbasis Role Based Access Control (RBAC) pada Sistem Informasi Akademik', *Jurnal Sistem Informasi Dan Teknologi*, 3(2), pp. 88–96.
- Pane, C. (2017) Analisis Yuridis Perlindungan Hukum terhadap Hak Wajib Pajak menurut Undang-Undang Ketentuan Umum dan Tata Cara Perpajakan Nomor 16 Tahun 2009. Universitas Medan Area. Available at: <https://repositori.uma.ac.id/jspui/bitstream/123456789/11761/1/141803065> - Charles Pane - Fulltext.pdf.
- Pramudya, A. (2019) 'Tren Serangan Cyber terhadap Data Pribadi Wajib Pajak di Indonesia', *Jurnal Keamanan Cyber Indonesia*, 5(2), pp. 45–56.
- Prasetyo, A. and Wahyudi, A. (2021) 'Dampak pelanggaran data pribadi terhadap reputasi instansi pajak di Indonesia', *Jurnal Manajemen Pajak*, 3(1), pp. 25–34.
- Pratama, B. (2020) 'Integrasi Regulasi Pajak dan Perlindungan Data Pribadi dalam Administrasi Pajak: Tinjauan dari Perspektif Kebijakan Publik', *Jurnal Ilmiah Administrasi Publik*, 7(1), pp. 45–60.
- Pratama, R.A. and Kurniawan, R. (2020) 'Penerapan Enkripsi Data untuk Keamanan Penyimpanan Informasi Pajak', *Jurnal Keuangan dan Teknologi Informasi*, 8(1), pp. 78–89.
- Rolamdo, J. and Widiastuti, N.P.E. (2021) 'Efektivitas Pengendalian Internal Pemungutan Pajak Reklame pada Unit Pelayanan Pemungutan Pajak Daerah Kelapa Gading', *Perspektif Akuntansi*, 4(3), pp. 255–276. Available at: <https://doi.org/10.24246/persi.v4i3.p255-276>.
- Rosid, A. (2016) A critical review of research design of qualitative and mixed-method approach papers in taxation, *Thoughts on Taxation, Life and Law*. Available at: <https://arifinrosid.com/2016/01/03/a-critical-review-on-research-design-of-qualitative-and-mixed-method-approach-papers-in-taxation/> (Accessed: 5 September 2024).
- Rulandari, N. et al. (2022) 'Analysis of the Effectiveness of Taxpayer Data Security in Implementing Tax Obligations at the Directorate General of Taxes', *Journal of Governance and Public Policy*, 9(3), p. Progress. Available at: <https://doi.org/10.18196/jgpp.v9i3.15976>.
- Sari, R. and Wibowo, A. (2019) 'Keadilan, Transparansi, dan Otonomi dalam Pengumpulan Data Pribadi', *Jurnal Administrasi Pajak*, 3(2), pp. 45–56.
- Septia, V. and Supriyo, A. (2023) 'Perlindungan Hukum terhadap Kerahasiaan Data Pribadi Wajib Pajak Daerah di Badan Pendapatan Daerah Kota Surabaya', *Mendapo: Journal of Administrative Law*, 4(2), pp. 176–195. Available at: <https://doi.org/10.22437/mendapo.v4i2.25206>.
- Setyawan, H. (2023) Jaminan Kerahasiaan atas Data dan Informasi Wajib Pajak, Beranda Komite Pengawas Perpajakan. Available at: <https://komwasjak.kemenkeu.go.id/in/post/jaminan-kerahasiaan-atas-data-dan-informasi-wajib-pajak-> (Accessed: 5 September 2024).
- Siregar, C. (2021) 'Perlindungan Privasi Data Pribadi Wajib Pajak: Tinjauan Etika dan Hukum', *Jurnal Pajak dan Etika Bisnis*, 15(1), pp. 102–115.
- Siswanto, H. and Tampubolon, A. (2019) 'Analisis biaya keamanan informasi pada sistem informasi pajak elektronik', *Jurnal Teknologi Informasi dan Ilmu Komputer*, 6(1), pp. 57–64.
- Sudjana, S.- (2022) 'Pembocoran Rahasia Bank sebagai Pelanggaran Hak Privasi dan Data Pribadi Elektronik Nasabah Bank', *Refleksi Hukum: Jurnal Ilmu Hukum*, 6(2), pp. 247–266. Available at: <https://doi.org/10.24246/jrh.2022.v6.i2.p247-266>.
- Sukmawati, A. (2019) 'Implementasi Undang-Undang Perlindungan Data Pribadi dalam Sistem Administrasi Pajak di Indonesia', *Jurnal Hukum dan Pembangunan*, 16(2), pp. 127–142.
- Susanto, B. and Hartono, D. (2020) 'Kepatuhan terhadap Regulasi Perlindungan Data Pribadi Wajib Pajak: Tantangan dan Strategi', *Jurnal Pajak dan Administrasi*, 7(1), pp. 12–25.
- Susanto, D. (2020) 'Implementasi Sistem Keamanan Informasi Terintegrasi dalam Administrasi Pajak', *Jurnal Keamanan Informasi*, 12(3), pp. 78–89.
- Tenny, S., Brannan, J.M. and Brannan, G.D. (2022) Qualitative Study, *National Library of Medicine*. Available at: <https://www.ncbi.nlm.nih.gov/books/NBK470395/> (Accessed: 5 September 2024).

- Utama, I.W.S. and Widianara, I.N. (2017) 'Pemantauan Aktivitas sebagai Upaya Pencegahan Kebocoran Data Pajak', *Jurnal Manajemen Teknologi*, 4(2), pp. 87–98.
- Utami, D.A. and Widyawati, I. (2021) 'Analisis Penggunaan Data Pribadi Siswa Dalam Penerapan Sistem Informasi Manajemen Sekolah', *Jurnal Sistem Informasi Dan Komputer*, 2(1), pp. 45–51.
- Wohrer, V. (2018) *Data Protection and Taxpayers' Rights: Challenges Created by Automatic Exchange of Information*. 1st edn. Amsterdam: IBFD. Available at: https://www.ibfd.org/sites/default/files/2021-12/18-066-Data-Protection-Taxpayers-Rights_final-web.pdf.