TABELLIUS Journal of Law
ISSN 2988-6201
published by
Master of Notarial Law
Faculty of Law
Universitas Islam Sultan Agung
Semarang

Legal Protection for the Confidentiality of Taxpayer Data in the Validation Process via E-PHTB Notary/Ppat

Nadila Marta Supriyanti[1)] & Jawade Hafidz[2)]

[1)] Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: nadilaxmm2@gmail.com

[2)] Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: jawade@unissula.ac.id

Abstract. *This research aims to find out and analyze the legal protection of taxpayers' personal data provided by the DJP as the organizer of the e-PHTB Notary/PPAT system. The approach method in this research is the statutory approach. The research specifications are descriptive data analysis required including secondary data taken using the literature study method. The data analysis method uses normative analysis. Based on researchconcludedthat legal protection for the personal data of e-PHTB Notary/PPAT taxpayers is protected in various laws, especially the Personal Data Protection Law. The DGT is obliged to operate electronic systems in a reliable, safe and responsible manner, has principles in processing personal data, and the need for the government to encourage the protection of personal data.*

Keywords: *Legal protection; Personal data; E-PHTB Notary/PPAT*

1. Introduction

In a sale and purchase transaction of land, whether accompanied by buildings or not, an exchange of ownership occurs. In this case, the land buyer will get ownership rights to the land and the land seller will get income in the form of money from payments for the land. Therefore, both sellers and buyers have their respective obligations. Buyers are required to pay Land and/or Building Rights Acquisition Fees (BPHTB). Meanwhile, sellers are required to deposit Income Tax (PPh) from the Transfer of Land and/or Building Rights (PHTB).[1]

[1]enforceA, E-PHTB makes SSP validation easier,https://enforcea.com/insight/e-bphtb-mudahkan-validasi-ssp, accessed on May 4, 2023 at 16.40.

Additional economic value obtained from the sale of land or buildings is subject to Tax on Acquisition of Land and Building Rights based on Law Number 1 of 2022 concerning Financial Relations between the Central Government and Regional Governments. BPHTB levies are closely related to the transfer of ownership of land rights because PPAT can only sign a deed of transfer of land and/or building rights after the taxpayer provides proof of tax payment.[2]PPAT has a significant role in checking BPHTB payments before making a sale and purchase deed. Payment of BPHTB tax is the obligation of the Taxpayer. After making the tax deposit, a formal research request is carried out which aims to ensure the completeness of the data in the form or application letter submitted by the Taxpayer. After seeing the phenomena that occur in the formal research request process, DJP tries to help the parties to carry out their obligations more easily while still paying attention to other aspects. July 14 2022 is the momentum for DJP to release a new application intended for Notaries/PPATs to submit formal research requests for Transfer of Rights and PPJB transactions which previously could only be carried out by sellers.[3]

Initially this application letter was submitted directly to the Tax Service Office, however since the introduction of the e-PHTB service now formal research requests can be submitted by a Notary and/or PPAT as regulated in Article 1 paragraph (3) of the Director General of Taxes Regulation No. PER-08/PJ/2022. The e-PHTB service is an online service for validating PPh PHTB Tax Payment Letters which is intended to make it easier for Taxpayers to validate the fulfillment of PPh payment obligations on the Transfer of Assets in the form of Land and/or Buildings. This service is aimed at providing legal certainty regarding the procedures for researching proof of PPh deposits for the transfer of PHTB and binding sale and purchase agreements for land or buildings so as to increase partnerships and cooperation with Notaries and/or PPAT. However, the authority of the Notary and/or PPAT in accessing e-PHTB means that the state official has the personal data of the Taxpayer. Notaries and/or PPATs are responsible for maintaining the confidentiality of taxpayers' personal data in accordance with Article 6 paragraph (5) of the Director General of Taxes Regulation No. PER-08/PJ/2022.

Taxpayer secrets must be protected. Because it will have certain impacts if the Taxpayer feels that his secrets are not protected and guarded. The impact that

[2]Azalia Delicia Dumanauw & Febby Mutiara Nelson, 2023, Legal Relationships That Arise in the Deposit of Land Sale and Purchase Tax Money to Land Deed Officials, in Jurnal Kertha Semaya, Vol 11 No. 8 of 2023 p. 1835-1847, Faculty of Law, University of Indonesia p. 1836,https://ojs.unud.ac.id/index.php/kerthasemaya/article/download/101796/50226/, accessed on May 4, 2023 at 17.00.

[3]Batam Tax Consultant, With e-PHTB Makes PPAT Notary Work Easier,https://www.ladfanidkonsultindo.com/2022/08/13/dengan-e-phtb-buat-kerja-notaris-ppat-cepat-mudah/, accessed on May 4 at 17.05

may arise is the taxpayer's reluctance to submit any data or information regarding themselves, their assets and business activities openly, honestly and without feelings of misgivings.[4]This matter should receive adequate attention, considering the importance of taxpayer secrets. The rapid development of communication technology can have an impact on the vulnerability of data leaks and misuse of information. *Where in the application published by the DJP iselectronic system or what could be called an online service, so all data is stored digitally and can be accessed online, this will be a particular vulnerability to the security of the stored data. Therefore, of course it must be balanced with adequate cyber security improvements.*

Data leaks often occur as technology advances and personal data protection is not followed. The confidentiality of personal data is very important for taxpayers considering that in 2022 a number of personal data leaks will occur through government websites.[5] This is not the first time personal data has been leaked. Apart from the government, personal data leaks have also been experienced by private companies in Indonesia. Since 2020, at least five cases of personal data leakage have been exposed to the media, including 230 thousand data on Covid-19 patients in Indonesia, 2.3 million KPU data, 1.2 million Bhinneka consumers, 13 million Bukalapak accounts, up to 91 million Tokopedia account.[6]

So it is important for electronic system administrators to pay attention to protecting personal data. Electronic system operators are obliged to protect personal data when processing personal data. Protection of personal data starts from obtaining and collecting, processing and analyzing, storing, correcting and updating, displaying, announcing, transferring, disseminating or disclosing, and/or deleting or destroying.

The issue of personal data leakage does not only occur with personal data managed by corporations or the private sector, but also Indonesian government institutions. The purpose of this personal data breach is to gain financial gain, either by reselling personal data, or misuse of personal data which is financially detrimental to the data owner. Several steps to protect personal data are needed by increasing public awareness and caution regarding data protection and modes of collection and breach of personal data.

---

[4]Gatot Faisal, 2007, How To Be A Smarter Taxpayer, Grasindo, Jakarta, p. 56.

[5]CNN Indonesia, 2022, Director General of Taxes Opens Voice on Alleged User Data Leaks" accessed viahttps://www.cnnindonesia.com/economic/20220303194435-78-766446/dirjen-pajak-buka-besar-soal-dugaan-data-user-bocoraccessed on May 4, 2023 at 20.30.

[6]House of Representatives of the Republic of Indonesia, 2021, Legislators Request Complete Investigation of Data Leak of 279 Million Population,https://www.dpr.go.id/berita/detail/id/33000/t/Legislator%20Minta%20Usut%20Tuntas%20Kasus%20Kebocoran%20Data%20279%20Millions%20Population, accessed on May 4, 2023 at 21.00.

Bearing in mind the dilemma as described above, the application published by the DJP is an electronic system, so all data stored digitally can be accessed online. This will be a particular vulnerability to the security of stored data. The aim of this research is to find out and analyze the legal protection of taxpayer data provided by the Directorate General of Taxes as the organizer of the e-PHTB Notary/PPAT system.

2. Research Method

This research uses mlegislative approach method.Research specifications useddescriptive analysis.The data used includes datasecondary.Retrieval of library material data.Using methodliterature review.Data analysis usingnormative analysis.

3. Results and Discussion

By looking at the vulnerabilities that occur in the security of electronic systems, researchers of course we are worried and question why these incidents often occur and it seems like there is no law enforcement. All incidents of personal data leakage seem to be resolved simply by reporting. It is as if corporations and related agencies are sufficient to inform the public by simply issuing statements and clarifications, as if the perpetrators of personal data theft are walking around freely carrying out these actions and as if they feel it is legal to be free to buy and sell personal data as a means of their livelihood by making offers through darknet sites. .[7]

Of course, a data leak incident may not only occur due to attacks from outside, because it may be an act of disclosure from within the organization itself. To clarify this, of course proof is needed which cannot depend solely on the statement of one party, but must also be proven by audits from other parties or related agencies. The government, through sectoral agencies in accordance with the authority granted by law, has the duties and functions and authority to supervise the protection of the public's personal data.

Historically, the terms privacy and personal data are actually nothing new. Even though the International Covenant on Civil and Political Rights (ICCPR) does not explicitly mention the term 'personal data', substantially the protection of personal data is part of everyone's privacy or personal life. Protection of personal data is not only regulated in the European Union regional convention (General Data Protection Regulation/GDPR), but also in other regions such as Africa (African Union Convention on Cyber Security and Personal Data Protection) and also Asia. In the ASEAN Declaration of Human Rights (2012) it is explicitly stated

[7]Faculty of Law, University of Indonesia, Legal Responsibility for Personal Data Leaks,https://law.ui.ac.id/percepatan- Hukum-terhadap-kebocoran-data-personal-oleh-edmon-makarim/, accessed on October 30, 2023 at 12:20.

that personal data is part of privacy, although it is not explained in more detail, in article 12 "No one may have his personal affairs, his family, his household or his correspondence arbitrarily disturbed; nor are they permitted to violate their honor and good name. Everyone has the right to legal protection against harassment or violations like this."

In Indonesia itself, philosophically, respect for privacy should also be understood as an embodiment of the second principle of Pancasila, namely Just and Civilized Humanity. The terms privacy and personal data have also been known and included since their existence UU no. 39 of 1999about human rights. Furthermore, 'personal data' is also mentioned and regulated in various subsequent laws and regulations, such as:[8]

1. UU no. 24 of 2013 about Population Administration

This law regulates the rights and obligations of residents, the authority of organizers and implementing agencies, population registration, civil registration, population data and documents, population information and administration systems, protection of residents' personal data, administrative sanctions and criminal sanctions related to population administration. Every Resident is obliged to report Population Events and Important Events they experience to the Implementing Agency by fulfilling the requirements required in Population Registration and Civil Registration.

2. UU no. 43 of 2009 about Archives

This law regulates: protection of civil rights and intellectual property rights as well as supporting the orderliness of State administration activities, storing and protecting the archives of individuals, families, political organizations and social organizations respectively in accordance with the standards and provisions of statutory regulations.

3. UU no. 11 of 2008 concerning Information and Electronic Transactions (UU ITE)

This law regulates various aspects of the use of information technology and electronic transactions, including the rights and obligations of internet users, protection of personal data, criminal actions related to misuse of information technology, and procedures for resolving electronic disputes.

4. Law Number 27 of 2022 concerning Personal Data Protection (UU PDP)

This law regulates the principles; type of personal data; rights of personal data subjects; processing of personal data; obligations of personal data controllers

[8]Ibid.

and personal data processors in processing personal data; transfer of personal data; administrative sanctions; institutional; international cooperation; society participation; dispute resolution and procedural law; prohibitions on the use of personal data; and criminal provisions related to the protection of personal data. Personal Data Protection is the overall effort to protect Personal Data in the process of Personal Data processing in order to guarantee the constitutional rights of Personal Data subjects.

5. Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions.

This law regulates the approach to regulating the criteria and boundaries of public and private PSE, and regulates the placement of data centers and PSE systems in a more measurable and definite manner that eliminates doubts about their obligation to register.

6. Government Regulation Number 80 of 2019 concerning Trading via Electronic Systemsk

This law regulates industrial activities*e-commerce*in Indonesia and is oriented towards consumer protection, however there are still several provisions that need to be clarified by the government in its implementation, for example through implementing regulations, with the spirit of supporting the development of e-commerce and protecting PMSE Business Actors.

In administering the electronic system, DJP as the owner of the e-PHTB Notary/PPAT application has the following obligations:[9]

1. Administering electronic systems reliably, safely and responsibly;
2. Do not contain and/or facilitate the distribution of electronic information/documents that are prohibited by law;
3. Carry out electronic system registration;
4. Implementing the principles of personal data protection;
5. Delete irrelevant electronic information/documents;
6. Managing, processing and storing electronic systems/data in Indonesia by Public Scope PSE;

[9]Directorate General of Informatics Applications, Government Regulations for the Implementation of Electronic Systems and Transactions (PP PSTE),https://aptika.kominfo.go.id/2019/08/peraturan-Pematuran-pste-no-82-tahun-2012/, accessed on October 30, 2023 at 12.30.

7. Providing access for supervision and law enforcement by Private Scope PSE;

Leakage of personal data processed/managed by the system administrator, in this case if it occurs in the e-PHTB Notary/PPAT system, whether due to hacking by a third party or intentionally leaked to a third party/public, is the responsibility of the system administrator as the personal data controller. Several principles that apply when personal data controllers process personal data, contained in Article 16 paragraph (2) of the PDP Law include:

1. Collection of personal data is carried out in a limited and specific manner, is legally valid and transparent;
2. The processing of personal data is carried out in accordance with its purpose;
3. The processing of personal data is carried out by guaranteeing the rights of the personal data subject;
4. The processing of personal data is carried out accurately, completely, not misleadingly, up to date and responsibly;
5. Processing of personal data is carried out by protecting the security of personal data from unauthorized access, disclosure, modification, misuse, destruction and/or deletion of personal data;
6. The processing of personal data is carried out by notifying the purposes and activities of the processing, as well as the failure to protect personal data;
7. Personal data is destroyed/deleted after the retention period ends at the request of the personal data subject, unless otherwise determined by statutory regulations; And
8. Processing of personal data is carried out responsibly and can be clearly proven.

Based on the provisions above, basically personal data controllers or system administrators have an obligation to prevent personal data leaks by protecting the security of personal data from unauthorized access, disclosure, modification, misuse, destruction and deletion of personal data.[10]

The following is the impact of hacking personal data on the affected system administrators:

[10]Online.com Law, E-Commerce Responsibility for Personal Data Leakage,https://www.Hukumonline.com/klinik/a/respons-respons-ie-commerce-i-atas-kebocoran-data-personal-lt63638331d18f0, accessed on 02 November 2023 at 09.00.

1. *Operational Down time* (Operational Cessation):

Operations may need to be halted completely until investigators get all the answers they need.

2. *Legal Liabilities* (Legal Obligations):

Organizations and countries are considered negligent in protecting personal data, potentially causing legal disputes.

3. *Business Reputation* (Business Reputation):

The victims of hacking its reputation and trust fall on users, investors and governments

4. *Lost Productivity* (Productivity Lost):

Loss of productivity, ideas, innovations taken over by competitors

5. *Financial Loss* (Financial Losses):

A lot of money was spent on researching the case, implementing new security systems and compensation costs.

If a personal data leak occurs, the system organizer concerned is obliged to provide written notification no later than 3x24 hours to its users and the institution that maintains personal data. The notification must contain the personal data that was disclosed, when and how the personal data was leaked, as well as efforts to handle and recover personal data leaks. If the leak of personal data disrupts public services and/or has a serious impact on public interests, then the system administrator must announce the leak to the public.[11]

In Article 57 paragraphs (1) and (2) of the PDP Law, personal data controllers who do not announce personal data leaks that have occurred may be subject to administrative sanctions in the form of:

1. Written warning;
2. Temporary suspension of all personal data processing activities;
3. Deletion or destruction of personal data; and/or
4. Administrative fines are imposed at a maximum of 2% of annual income or annual receipts for variable violations.

[11]Hukum Online.com, BPJS Responsibility for Leaks of Participants' Personal Data,https://www.Hukumonline.com/klinik/a/respons-respons-bpjs-atas-kebocoran-data-personal-pesertanya-lt6389d13f91363/, accessed on 02 November 2023 at 09.10.

In this case, users can report to a special agency that organizes personal data protection which will later be determined by the president. The authority of the Institution is as follows:

1. Formulate and establish policies in the field of PDP;
2. Supervise personal data controller compliance;
3. Imposing administrative sanctions for PDP violations;
4. Assist law enforcement officials in handling suspected personal data crimes as intended in the law;
5. Cooperate with other countries' personal data protection agencies in the context of resolving alleged cross-border PDP violations;
6. Carry out an assessment of the fulfillment of requirements for the transfer of personal data outside the jurisdiction of the Republic of Indonesia;
7. Give orders to follow up on monitoring results to personal data controllers and/or personal data processors;
8. Publicize the results of the implementation of PDP supervision in accordance with statutory provisions;
9. Receive complaints and/or reports regarding alleged PDP violations;
10. Carrying out examinations and resolution of complaints, reports and/or monitoring results regarding alleged PDP violations;
11. Summon and present every person and/or public body related to alleged PDP violations;
12. Request information, data, information and documents from any person and/or public body regarding alleged PDP violations;
13. Summon and present the necessary experts in the examination and investigation regarding suspected PDP violations;
14. Carrying out inspections and searches of electronic systems, facilities, spaces and/or places used by personal data controllers and/or personal data processors, including obtaining access to data and/or appointing third parties; And
15. Request legal assistance from the prosecutor's office in resolving PDP disputes.

Therefore,as explained in article 60 of the PDP Law, this institution has the authority to formulate andestablish policies in the field of personal data protection, carry out supervision ofpersonal data controller compliance, up to imposing administrative sanctions for violations of personal data protection committed by personal data controllers and/or personal data processors. Apart from that, this agency also has the authority to assist law enforcement officers in handling casesalleged personal data criminal offenses as intended in the PDP Law and collaborating with other countries' personal data protection agencies in the context of resolving alleged cross-border personal data protection violations.

Apart from administrative sanctions, for leakage of consumer data or in this case the system operator, the aggrieved user can be sued civilly. This is regulated in Article 12 paragraph (1) of the PDP Law which states that personal data subjects (users) have the right to sue and receive compensation for violations of personal data processing in accordance with statutory provisions. Users or consumers who are harmed by data leaks can sue under Article 1365Civil Coderegarding unlawful acts.

Personal data controllers are obliged to maintain the confidentiality of personal data and must be responsible for fulfilling obligations to implement the principles of personal data protection as explained in Article 36 which states "In processing Personal Data, Personal Data Controllers are obliged to maintain the confidentiality of Personal Data" and in Article 47 which states "Personal Data Controllers must be responsible for the processing of Personal Data and show responsibility for implementing the principles of Personal Data Protection." DJP as the controller of personal data is obliged to comply with the regulations in the PDP Law.

In this case, if personal data in the form of KTP identity is distributed by irresponsible individuals, it can be subject to Article 65 paragraph (2) in conjunction with Article 67 paragraph (2) of the PDP Law which confirms that "Every person is prohibited from unlawfully disclosing Personal Data that does not belong to him." ” and “Any person who deliberately and unlawfully discloses Personal Data that does not belong to him as intended in Article 65 paragraph (2) shall be punished by a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000 (four billion rupiah).

As for hackers who steal personal data, they can be subject to sanctions as stipulated in The PDP Law itself stipulates criminal sanctions for the following actions:

1. Any person who intentionally and unlawfully obtains or collects personal data that does not belong to him with the intention of benefiting himself or another person which may result in loss to the subject of personal data will be

sentenced to imprisonment for a maximum of 5 years and/or a fine of a maximum of IDR 5 billion.

2. Any person who intentionally and unlawfully discloses personal data that does not belong to him or her will be sentenced to imprisonment for a maximum of 4 years and/or a fine of a maximum of IDR 4 billion.

3. Any person who intentionally and unlawfully uses personal data that does not belong to him or her will be sentenced to imprisonment for a maximum of 5 years and/or a fine of a maximum of IDR 5 billion.

4. Any person who deliberately creates false personal data or falsifies personal data with the intention of benefiting themselves or others which could result in harm to others will be sentenced to imprisonment for a maximum of 6 years and/or a fine of a maximum of IDR 6 billion.

Based on the provisions above, the criminal act of theft of personal data (identity theft) can be charged using Article 67 paragraphs (1) and (3) of the PDP Law, namely with the threat of a maximum prison sentence of 5 years and/or a maximum fine of IDR 5 billion.

Apart from being sentenced to a criminal sentence, the perpetrator can also be sentenced to additional punishment in the form of confiscation of profits and/or assets obtained or proceeds from criminal acts and payment of compensation. Meanwhile, if the theft of personal data is carried out by a corporation, then the crime in Article 67 of the PDP Law can be imposed on the management, control holder, order giver, beneficial owner and/or corporation (specifically a fine).

Even though criminal sanctions have been specifically regulated in the PDP Law, the procedural law applicable in the criminal justice process regarding the protection of personal data still refers to the provisions in the Criminal Procedure Code.

There are many incidents of crimes against electronic systems carried out by attackers, to control other people's accounts there are several ways, such as:[12]

1. *Phishing*

The crime is committed by trapping the victim using a fake login page that is made to appear similar to the original login page

2. *Social Engineering*

[12]Directorate General of Informatics Applications, Electronic System Operators Responsible for Data Breaches,https://aptika.kominfo.go.id/2020/06/pengelenggara-sistem-elektronik-besar-terhadap-pelanggaran-data/, accessed on 02 November 2023 at 09.15.

Crimes committed by approaching the victim with the aim of manipulating the victim so that they will unknowingly follow the perpetrator's instructions or provide what the perpetrator asks for.

3. *Guest Password*

Crimes committed manually or using tools to guess passwords. Usually victims of password guesting techniques use weak passwords

Implementations that can be carried out to protect the Personal Data of system users, namely:

1. Government Calls for Increased Protection of Personal Data

In various countries, issues related to privacy and privacy regulations have begun to develop as part of the development of society in the digital era. Currently, the PDP Law has become a more comprehensive legal umbrella for personal data protection and can provide guarantees for the protection of personal data for the public. However, the existence of adequate regulations is not enough without digital awareness and literacy. Digital literacy plays an important role in efforts to increase personal data protection. There are three easy steps you can take to maintain the security of personal data, namely, be careful when giving approval or pressing links whose source is not clear, don't save all passwords on cellphones or other devices that are not properly encrypted, and third, be critical of various requests. data, we reserve the right to refuse requests for irrelevant data.[13]

2. VIDA's role as PSrE is under Kominfo

As an Electronic Certificate Provider (PSrE), VIDA helps the government's mission in creating a safe digital ecosystem in Indonesia. VIDA guarantees the security of consumers' personal data in online identity verification process services through world-class technology and standards. Armed with a VIDA electronic certificate, the decision to authenticate digital services or the electronic signature process rests entirely with the user. VIDA protects user personal data and uses it only for user purposes, by implementing end-to-end encryption for all data transmissions. As PSrE under Kominfo, VIDA has the legality and validity of electronic signatures in the eyes of the law and the courts. VIDA is the first PSrE in Indonesia to obtain global WebTrust accreditation for implementing internet security standards and the first PSrE from Indonesia to be included in the Adobe Approved Trust List (AATL) or Adobe's list of trusted partners. In providing online identity verification

[13]Vida, Implementation of Personal Data Protection in Indonesia,https://vida.id/id/blog/implementation-of-personal-data-protection-in-indonesia, accessed on 02 November 2023 at 09.20.

services, VIDA is also listed as the organizer of the Digital Financial Innovation (IKD) e-KYC Cluster registered with the OJK and regulatory sandbox at the OJK.[14]

3. Maintaining State Sovereignty

The PDP Law is the legal basis for Indonesia to maintain state sovereignty, state security, and protect personal data belonging to Indonesian citizens. The scope of data protection according to the PDP Law is wherever personal data is located within the territory of the Republic of Indonesia, outside the territory of the Republic of Indonesia, the government, the public sector or the private sector.

One of the government's efforts to protect people's personal data and encourage awareness of PDP is by providing guidelines and derivative regulations. Then provide proper education and increase awareness of PDP through electronic media, print media or online media, as well as national and international collaboration.

Also developing the Data Protection Officer (DPO) ecosystem in the private sector and government agencies by preparing DPO training modules, establishing DPO competency standards and training and training institutions or DPOs for Ministries/Institutions and Provincial Governments.[15]

According to researchers, in providing legal protection for users and administrators of the e-PHTB Notary/PPAT system, it would be best for the DJP to form derivative regulations regarding legal protection in the implementation of the e-PHTB Notary/PPAT system. Currently the protection of Personal Data is regulated in the Personal Data Protection Law, but the government needs to encourage the public to be aware of personal data, and also the need to maintain a good information system by establishing a personal data protection agency. In particular, DJP as the organizer of the e-PHTB Notary/PPAT system needs to have experts who can handle personal data protection.

Based on the protection provided, legal protection for taxpayers and notaries/PPATs is in accordance with Setiono's theory of legal protection. Setiono's opinion regarding legal protection is an action or effort to protect society from arbitrary actions by authorities that are not in accordance with the rules of law. And functions to create order and tranquility so as to enable humans to enjoy their dignity as human beings.

[14]Ibid.

[15]Directorate General of Informatics Applications, Protect Personal Data Leaks Here are the Preventive Measures,https://aptika.kominfo.go.id/2020/08/lindungi-kebocoran-data-personal-ini-aksi-pengcepatannya/, accessed on 02 November 2023 at 09.30.

4. Conclusion

In providing legal protection for taxpayers' personal data in the validation process on the PPAT/Notary e-PHTB system, DJP as the system organizer has the duties and functions as well as the authority to supervise the protection of taxpayers' personal data. Personal Data is also mentioned and regulated in various laws and regulations, such as:UU no. 24 of 2013about Population Administration;UU no. 43 of 2009about Archives;UU no. 11 of 2008concerning Information and Electronic Transactions (UU ITE); Law Number 27 of 2022 concerning Personal Data Protection (UU PDP); Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions; and Government Regulation Number 80 of 2019 concerning Trading via Electronic Systems. In protecting Taxpayers' Personal Data, the DGT as the system organizer needs to follow the following principles of personal data protection: Processed according to lawfulness, fairness and transparency; Limiting the purposes of data collection (Purpose Limitation); Minimize data collection (Data Minimisation); Data must be accurate and always updated (Accuracy); Only store data that is still in accordance with the purpose of data collection (Storage Limitation); Always maintain the integrity and confidentiality of data (Integrity and Confidentiality) and all principles are implemented by showing a sense of responsibility in protecting data (Accountability). There are implementations that can be carried out to protect the Personal Data of system users, as follows: 1. The role of the government in calling for increased protection of personal data with the formation of the PDP Law as a legal umbrella for the public regarding their personal data, but this is not enough without digital literacy that can plays an important role in efforts to increase data protection of personal data; 2.Encouraging awareness of Personal Data Protection, namely byprovide guidelines and derivative rules. Then provide proper education and increase awareness of PDP through electronic media, print media or online media, as well as national and international collaboration. Also developing the Data Protection Officer (DPO) ecosystem in the private sector and government agencies by preparing DPO training modules, establishing DPO competency standards and training and training institutions or DPOs for Ministries/Institutions and Provincial Governments. In order to provide legal protection for Personal Data, it is necessary for the Directorate General of Taxes to form regulations regarding legal protection for the implementation of e-PHTB Notary/PPAT. The government is firmly expected to immediately establish a personal data protection agency as the implementer and supervisor of the PDP Law.Establishing a personal data protection body that is independent and free from the influence of any institution is crucial and cannot be ruled out. This is important because later this institution will also supervise the management of public service data managed by government institutions and also the management of private or private service data.

5. References

Journal and Internet Resources

CNN Indonesia, 2022, Director General of Taxes Opens Voice on Alleged User Data Leaks, accessed viahttps://www.cnnindonesia.com/economic/20220303194435-78-766446/dirjen-pajak-buka-besar-soal-dugaan-data-user-bocor, accessed on May 4, 2023 at 20.30.

House of Representatives of the Republic of Indonesia, 2021, Legislators Request Complete Investigation of Data Leak of 279 Million Population,https://www.dpr.go.id/berita/detail/id/33000/t/Legislator%20Minta%20Usut%20Tuntas%20Kasus%20Kebocoran%20Data%20279%20Millions%20Population, accessed on May 4, 2023 at 21.00.

Directorate General of Informatics Applications, Protect Personal Data Leaks Here are the Preventive Measures,https://aptika.kominfo.go.id/2020/08/lindungi-kebocoran-data-personal-ini-aksi-pengcepatannya/, accessed on 02 November 2023 at 09.30.

Directorate General of Informatics Applications, Electronic System Operators Responsible for Data Breaches,https://aptika.kominfo.go.id/2020/06/pengelenggara-sistem-elektronik-besar-terhadap-pelanggaran-data/, accessed on 02 November 2023 at 09.15.

Directorate General of Informatics Applications, Government Regulations for the Implementation of Electronic Systems and Transactions (PP PSTE),https://aptika.kominfo.go.id/2019/08/peraturan-Pematuran-pste-no-82-tahun-2012/, accessed on October 30, 2023 at 12.30.

Dumanauw Delicia Azalia & Nelson Mutiara Febby, 2023, Legal Relationships That Arise in the Deposit of Land Sale and Purchase Tax Money to Land Deed Officials, in JurnalKertha Semaya, Vol 11 No. 8 of 2023 p. 1835-1847, Faculty of Law, University of Indonesiap. 1836https://ojs.unud.ac.id/index.php/kerthasemaya/article/download/101796/50226/, accessed on May 4, 2023 at 17.00.

enforceA, E-PHTB makes SSP validation easier,https://enforcea.com/insight/e-bphtb-mudahkan-validasi-ssp, accessed on May 4, 2023 at 16.40.

Faculty of Law, University of Indonesia, Legal Responsibility for Personal Data Leaks,https://law.ui.ac.id/percepatan- Hukum-terhadap-kebocoran-data-personal-oleh-edmon-makarim/, accessed on October 30, 2023 at 12:20.

Hukum Online.com, BPJS Responsibility for Leaks of Participants' Personal Data,https://www. Hukumonline.com/klinik/a/respons-respons-bpjs-atas-kebocoran-data-personal-pesertanya-lt6389d13f91363/, accessed on 02 November 2023 at 09.10.

Online.com Law, E-Commerce Responsibility for Personal Data Leakage,https://www. Hukumonline.com/klinik/a/respons-respons-ie-commerce-i-atas-kebocoran-data-personal-lt63638331d18f0, accessed on 02 November 2023 at 09.00.

Batam Tax Consultant, With e-PHTB Makes PPAT Notary Work Easier,https://www.ladfanidkonsultindo.com/2022/08/13/dengan-e-phtb-buat-kerja-notaris-ppat-cepat-mudah/, accessed on May 4 at 17.05.

Vida, Implementation of Personal Data Protection in Indonesia,https://vida.id/id/blog/implementation-of-personal-data-protection-in-indonesia, accessed on 02 November 2023 at 09.20.

Book

Faisal Gatot, 2007, How To Be A Smarter Taxpayer, Grasindo, Jakarta.