JOURNAL OF GOVERNANCE AND PUBLIC POLICY

Journal of Governance and Public Policy
ISSN: 2460-0164 (print), 2549-7669 (Online)
Vol 9, No 3 (2022): Page no: 241-254

Analysis of the Effectiveness of Taxpayer Data Security in Implementing Tax Obligations at the Directorate General of Taxes

Novianita Rulandari[1], Alian Natision[2], Victor Van Kommer[3] , Andri Putra Kesmawan[4], Suryanih[5]
[1] Institut STIAMI, Mobile +6281289935858, Indonesia
[2] Institut STIAMI, Mobile +6282111269869, Indonesia
[3] IBFD, Mobile +31611017939, Netherland
[4] Universitas Muhammadiyah Yogyakarta, Mobile +62818240698, Indonesia
[5] Institut STIAMI, Mobile +62895365901568, Indonesia
Corresponding Author: novianitarulandari@gmail.com

Article Info

Article History;
Received:
2022-08-24
Revised:
2022-09-14
Accepted:
2022-10-21

Abstract: Taxpayer data security in carrying out tax obligations at the Directorate General of Taxes has experienced several problems of taxpayer data leakage because the security system is still weak, so it is infected with malware that can steal taxpayers' data. This study aims to evaluate the effectiveness of taxpayer data security in carrying out tax obligations with case studies at the Directorate General of Taxes, knowing the obstacles faced by the Directorate General of Taxes in building a system for taxpayer data security information and analyzing the efforts made by the Directorate General of Taxes regarding the system for developing taxpayer data security in carrying out tax obligations. This study used a descriptive qualitative approach. Data collection was done through observation, interviews, documentation studies, and data analysis techniques using content analysis. The results indicated that after the taxpayer data leak, the Directorate General of Taxes implemented a comprehensive system improvement to improve taxpayer data security. The participation of taxpayers in using a solid username and password is an essential factor in determining the taxpayer's data. The Directorate General of Taxes seeks to improve the security system and provide socialization to taxpayers, always using usernames and passwords that are not easily guessed and changing E-filing passwords periodically.

Keyword: *Data Security Effectiveness; Information Systems; Taxpayer; E-filing.*

DOI: https://doi.org/10.18196/jgpp.v9i3.15976

INTRODUCTION

One current state revenue source is the tax sector (Fang et al., 2022; Kariyoto, 2012; Lin & Jia, 2019; Ndoricimpa, 2021). A developing country's taxes can provide advantages in recovering from the national economic crisis (Compaoré, 2022; Gavard et al., 2022; Matti et al., 2022). Tax is one of the main sources of revenue, which has a vital role for the state (Albram, 2016; Pohan, 2021; Setiowati et al., 2020). The revenue is useful for many aspects, such as implementation and development aimed at increasing the prosperity and welfare of the people. As one of the great potential sources of state revenue, revenue from the tax sector must continue to be increased (Dantes & Lasminiasih, 2021; Hapsari et al., 2018; Ratnawati, 2016). The government's efforts to increase state revenues from the tax sector are initiated by reforming the national tax system (Butarbutar, 2017; Marlina & Syahribulan, 2021; Samudra, 2016).

Information technology security is security management aiming to prevent, overcome and protect information technology from the risk of illegal actions (Bag & Wang, 2021; Reck et al., 2022; Xiao & Shao, 2020). The development of technology is currently experiencing many changes. These developmental technologies, supported by developing science, impact progress in the archives field (Binder & Haupt, 2022; Dong & Sinning, 2022; Fu et al., 2019).

Technology Acceptance Model (TAM) is the user's perception of a system that can affect the user's attitude (Rafique et al., 2020; Scherer et al., 2019). TAM is the recipient of a technology influenced by the benefits and ease of use (Al Hujran et al., 2013; Liu et al., 2022; Low et al., 2020; Megayani & Noviari, 2021). Theory of Reasoned Action (TRA) states that technology is influenced by a person's desire to use it, which is caused by user beliefs, namely the perception of the usefulness of a system and the perception of the ease of a system (Acharya & Mekker, 2022; Alnemer, 2022; Aziz & Idris, 2014).

An information system can be good if the system's security is reliable (K. Adi et al., 2018; Fernandes et al., 2017; Wiczorek & Zirk, 2019). System security can be seen through user data that is safely stored by the information system. If user data can be stored safely, it will minimize other parties' misuse of taxpayer data (Faúndez-Ugalde et al., 2020; Leroux & Pupion, 2022; Santoro, 2021). Taxpayer data must be confidential, and no third party can find out. Ease of technology can be defined as a measure by which individuals believe the technology system can be easily understood and used (Bahri & Listiorini, 2019; Situmeang, 2021). A system can be of high quality if the system is designed to meet user satisfaction through the ease of using the system (Bel et al., 2017; Castellón González & Velásquez, 2013).

The Directorate General of Taxes (DGT) ensures that DGT data, including taxpayer data, is kept by DGT in a safe condition. It was in response to a thread stating that as many as 49,000 leaked user credentials were used for logging into government websites. (Detik Finance, 2022; Purnomo, 2022; Said, 2022). The data leak is suspected of having come from a user's device infected with malware and then used to enter government sites. There was a leak from the user's side. Therefore, users of the tax.go.id website and taxpayers at large immediately replace the account password with a stronger and safer one, so they are not easily hacked. From the report, the Indonesian government is included in the list of the top 10 sites, one of which is through the Directorate General of Taxes website *(djponline.pajak.go.id).*

The governance of the collection and taxpayer data is regulated in the Decree of the Minister of Finance Number 878/KMK.01/2019 concerning the Policy on Governance of Tax Data Access Authority. Based on observations and pre-research interviews, several problems were identified, including (1) A leak of 49 thousand credential data; (2) An infected user's device with malware; (3) Not updated antivirus; (4) Weak and insecure passwords; (5) Passwords that are never changed; (6) Easy-to-identify passwords; (7) Ineffective use of e-filling; (8) Less flexible e-filling; (9) Taxpayers who do not understand the operation of e-filling; and (10) Lack of preparedness of taxpayers regarding information technology in using e-filling (Hifni, 2022; Setiawan, 2021).

In potential tax revenue in Indonesia, a strategy will further optimize its revenue and the security of taxpayers. From the strategy set, we can see if there is an effect related to the security of taxpayer data in paying taxes before and find out the obstacles faced in implementing taxpayer data security.

This study aims to evaluate the effectiveness of taxpayer data security in carrying out tax obligations with case studies at the Directorate General of Taxes, knowing the obstacles faced by the Directorate General of Taxes in building an information system for taxpayer data security and analyzing the efforts made by the Directorate General of Taxes regarding security system for development taxpayer data in carrying out tax obligations.

In the digital era, communication through computer networks plays an important role. Through electronic communication, a person can make transactions or communications very quickly and easily. It affects relatively significant developments in information technology, where the internet is getting bigger with cheaper access costs. The consequence is that the risk in information security is increasing.

Data security is the protection of data in a system against unauthorized authorization, modification, or destruction and the protection of computer systems against unauthorized use or modification.

There are four (4) main aspects regarding data and information security: (1) Privacy/Confidentially, which is an effort to protect personal information data from people who are not entitled to access; (2) Integrity is efforts to keep data or information from being changed by unauthorized persons; (3) Authentication, which is an effort or method to determine the authenticity of the information, for example, whether the information sent is opened by the right person or the service from the services provided is from the server in question, and (4) Availability, related to the availability of systems and data (information) when needed.

Effectiveness is a measure of the success or failure of an organization to achieve its goals. So the organization is said to have been running effectively. The most important thing to note is that effectiveness does not say how much it has cost to achieve this goal. (Mardiasmo). Other experts stated that effectiveness is using resources, facilities, and infrastructure in an amount consciously determined beforehand to produce the number of goods or services it carries out. Effectiveness shows success whether or not the targets have been achieved. If the activity results are closer to the target, the higher the effectiveness. Based on the above opinion, effectiveness is related to achieving a result.

The factors that can affect effectiveness are as follows: (1) Characteristics of the organization mean that relationships that are usually fixed, such as the arrangement of human resources, can be found in the organization. The structure is a way of putting people together to make up an organization. In it, humans are placed as part of a usually fixed relationship, and then a task-oriented interaction pattern is determined; (2) Characteristics of the environment in which there are two aspects, namely the internal environment and the external environment. The external environment itself is an environment that is outside an organization. While the internal environment is an environment that is entirely within the organization's environment, (3) The characteristics of these workers are factors that greatly influence effectiveness. Each individual will generally find many differences that influence the organization's goals. So if an organization wants to succeed in achieving its goals, then the organization must be able to integrate personal goals with the goals of the organization, and (4) Management characteristics are a strategy and work mechanism used to regulate all aspects of the organization until the effectiveness of existing plans or policies are achieved. To achieve organizational goals when implementing their policies, leaders must focus on their members, not only strategies and mechanisms.

Several previous studies regarding information systems in tax payments by taxpayers and E-Filing showed similar results, a positive and significant effect on the effectiveness of tax payment information systems by taxpayers through E-Filing on taxpayer compliance in carrying out tax obligations. (Fazri, 2017; Feng et al., 2022; Norzhela et al., 2019; Wardani et al., 2021; Wulandari, 2021). Factors such as ease of use and security of taxpayer data in using E-Filing have a positive and significant influence on taxpayer compliance and increased tax revenue for the state. (I. K. Y. Adi, 2020; Cappelletti et al., 2017; Chairani & Farina, 2021; Dewi, 2019). Several previous studies analyzed information technology in improving taxpayer compliance in Russia, Perancis, dan China (Fedotova et al., 2019; Leroux & Pupion, 2022; Yang et al., 2021).

RESEARCH METHOD

This study used a descriptive qualitative approach (Creswell, 2017; Sugiyono, 2019). Data collection techniques through observation, interviews, documentation studies, and data analysis techniques using content analysis (Arikunto, 2013; Moleong, 2018). The novelty factor that distinguishes this research from previous research is the approach and research method used. Previous studies only examined E-Filing information systems to increase taxpayer compliance and state revenues through taxes. At the same time, this research focuses on the factors that support and hinder efforts to use information technology in fulfilling tax obligations and the efforts made by the Directorate of Taxpayers to ensure that the information system used is understandable and safe against leaks, both internal and external. What distinguishes this research from previous research is the approach and research method used.

Previous studies only examined using information systems through E-Filing to increase taxpayer compliance and state revenues through taxes. In contrast, this research focuses on the factors that support and hinder efforts to use information technology in fulfilling tax obligations and the efforts made by the Directorate of Taxpayers to ensure that the information system used is understandable and safe against internal and external leaks.

RESULTS AND DISCUSSION

In conducting this research, the authors used a qualitative descriptive method with research instruments such as interviews, observations, and documentation. The answers given by the informants then interpreted the results of the research that the authors did, either through interviews or observing written data or documents related to the Effectiveness Analysis of Taxpayer Data Security in carrying out Tax Obligations. The research conducted by the authors, the results are as follows.

In this interview, the authors used an in-depth open interview. In-depth open interviews are conducted through a face-to-face stage, and only direct questions and answers between data collectors and researchers to informants or data sources. Interviews in this study need to be done because the authors will know more in-depth about the participants in interpreting the situations and phenomena. This in-depth interview was conducted with competent parties regarding the effectiveness of Taxpayer Data Security in Implementing Tax Obligations and the reality on the ground, among them; Tax Authorities, Taxpayers, and Academis.

The organization's characteristics in paying attention to the effectiveness of taxpayer data security are reflected in officers who are specifically responsible for maintaining the security of taxpayer data. Based on the results of interviews with all informants, it is known that the DGT has appointed a special officer or administrator who has the task of ensuring that taxpayer data is kept safe by limiting access to computer use and exchanging data using USB or Flashdisk, to avoid infection with dangerous computer viruses or malware. However, this officer was not properly socialized with all taxpayers, so one of the taxpayer informants stated that he did not know about officers who had special responsibilities to handle taxpayer data problems.

Human resources show organizational characteristics in the effectiveness of data security in carrying out obligations to improve taxpayer data security. Each KPP has a consul operator in charge of maintaining the security of taxpayer data. Consul operators are responsible for technically ensuring taxpayer data security, but the obligation to secure data is not only the responsibility of a consul operator. All tax authorities or tax officers must secure taxpayer data. To provide knowledge and skills regarding data security to consular operators and tax authorities, each KPP conducts special training on taxpayer data security. Several important aspects were emphasized during the training. For example, the tax authorities were prohibited from opening unknown emails to prevent the entry of viruses or malware via spam emails that could compromise the security of taxpayer data. In addition, the tax authorities are prohibited from leaving any documents on the table when leaving their work desk or office. All physical documents must be restored in a locked cabinet after use. All taxpayer informants agreed that the DGT must have competent resources in the field of information technology in order to maintain the security of taxpayer data. However, competence must also be a dissertation with credibility and a good work ethic, as well as having high integrity to participate in supporting and succeeding DGT's policies to increase tax revenues.

To improve the effectiveness of taxpayer data security, apart from providing human resources who are responsible for the security of taxpayer data, DGT has taken preventive measures in the field of information technology, such as making Standard Operating Procedures (SOP) for the use of computer networks and the internet when working. One is installing a firewall on the DGT server so that no one can access the taxpayer's data. The next step is to change passwords regularly using a password generator that is complex and difficult to break. The information system also has an automatic log-out protocol when the computer is not used within 60 seconds to prevent the use of the computer by irresponsible parties. The SOP also regulates the exchange of data between sections that must use administrator or consul officer access so that a tax officer cannot access data from other fields through his computer without the administrator's

permission. All tax authorities must implement this SOP without exception, and any violation of the SOP will be subject to sanctions in the form of a warning, warning letter, and even dismissal.

The problem of taxpayer data leakage was known from social media in March 2022, when one of the accounts on Twitter, Darktracer, released a list of 100 thousand government sites worldwide that had experienced data leaks through malware infections. One of the sites in Indonesia on the list is the Directorate General of Taxes website. Hackers have stolen over 40 thousand taxpayer data in Indonesia through malware that is infiltrated into the computers of taxpayers who access the DGT website. In addition to the DGT website, data theft was carried out on dozens of other government sites. DGT immediately investigated the matter and found that there were hacking attempts by certain taxpayer accounts that had been infected by malware or hijacked by hackers. However, the Taxpayer Data server at the DGT has a layered security system through a firewall, so hackers cannot enter the central server containing data on hundreds of millions of taxpayers in Indonesia. So it can be concluded that Darktracer's statement in his post on social media Twitter is a hoax or a hoax. So far, taxpayer data is stored and well-protected on the DGT server. Therefore, DGT urges taxpayers not to easily believe the news circulating on social media because it tends to be misleading. Informants from taxpayers were disappointed if the leak of taxpayer data was true and demanded that the DGT take full responsibility for the losses caused by the incident. Meanwhile, informants from academic circles stated that so far, taxpayer data is well protected on the DGT server. All hacking attempts on taxpayer data can be handled properly.

For this incident, the DGT then conducted a comprehensive information system security analysis to ensure that there were no security holes that irresponsible hackers could enter to steal taxpayer data on the DGT server. The DGT team also blocked the accounts of taxpayers suspected of having been hijacked and used to access the DGT website illegally. Furthermore, the DGT asked the taxpayer to re-verify by creating a new password via the taxpayer's email. One of the informants stated that taxpayer data could only be leaked by insiders or tax authorities with full access to taxpayer data. However, if the tax authorities do it, the penalty of dismissal is waiting for the tax authorities who commit the violation.

The possibility of leakage of taxpayer data on the DGT website from the external environment is still possible because hackers always try various ways to steal taxpayer data in Indonesia and then sell it at high prices in hacker forums on DarkNet. An informant from the DGT tax office stated that there had been a ransomware hack, but it did not have a significant impact and could be immediately addressed by the DGT's IT team. Informants from academics stated that the opportunity for taxpayer data to be leaked would always exist. However, it depends on how DGT, especially KPP, responds to this matter. Taxpayer data security system must be a special concern for each KPP by always updating the security system using the latest output. Every day, thousands of types of viruses, malware, and ransomware are created by hackers after studying the weaknesses of the security systems of certain institutions' websites. If the administrator at the KPP is negligent in updating the latest antivirus and firewall, the chances for leaks will be even greater. It is certainly not expected by the tax authorities and the taxpayers themselves. Therefore, DGT should ensure that DGT's information system and servers have the latest and best security systems to prevent data leakage.

In contrast to the possibility of leakage of taxpayer data from the external environment, the opportunity for leakage from the internal environment is much less likely to occur. It is because the risk of sanction that can be accepted by the Ficus who deliberately leaks data is heavy, which can lead to dismissal. Of course, this is not expected to happen by all tax authorities in DGT and KPP. In addition, as a State Civil Apparatus (ASN), they have also been sworn in to maintain the confidentiality of institutional data, in this case, hundreds of millions of taxpayer data throughout Indonesia. However, the possibility of leakage of taxpayer data in the internal environment of the DGT and KPP may still occur due to the unintentional negligence of the tax authorities. The DjP will investigate if it occurs, assess the losses incurred, and then decide what sanctions will be given to the tax authorities, whether verbal warnings, warning letters, or even immediate dismissal. Suppose the impact is very large and even endangers the national interest, then in addition to dismissal. In that case, the focus also faces criminal charges through the Electronic Information and Transaction Law (UU ITE), with a criminal penalty of up to 10 years.

Internally, DGT has a performance appraisal system for each taxpayer, and the results of the performance report from each tax office will be evaluated and audited by the inspectorate. Tax authorities who have poor performance or are indicated to have committed violations of misuse of taxpayer data or negligence in managing taxpayer data will be given guidance and verbal or written warnings. They can also be transferred to other departments or other KPP.

All tax authorities must have high integrity in their duties and functions according to their respective positions. The staffing system at the DGT does not open up opportunities for the tax authorities to violate the existing staffing regulations. Fiskus also understands the sanctions that can be accepted if they commit a deliberate violation, so each Fiskus is more focused on completing their respective duties and responsibilities. Indeed, there are still tax officers who violate the rules. However, the number is small compared to Indonesia's total number of tax officers. Every violation of the rules committed by the tax authorities can be ascertained that the tax authorities concerned have received sanctions for their actions.

In addition, the DGT also carries out coaching steps through training for each tax officer regarding their responsibilities in maintaining the confidentiality of taxpayer data, making SOPs regarding the use of taxpayer data, and regulating access to taxpayer data by each tax office. Fiskus were also warned against the sanctions they could receive if they intentionally or unintentionally leaked taxpayer data. This training is technically aimed at improving the competence of the tax authorities and morally increasing the credibility and integrity of the tax authorities towards the institution and their duties and authorities.

To anticipate the occurrence of taxpayer data leaks in the future, technically, the DGT updates the security system from the DGT server regularly, either daily, weekly, or monthly to prevent hacking from outside by irresponsible hackers. Meanwhile, to anticipate the occurrence of data leakage internally, DGT continues to conduct training and socialization regarding the importance of maintaining the security of taxpayer data because taxpayer data is legally protected personal data. Then technically, every tax officer is prohibited from copying taxpayer data using external storage such as flash disks, compact disks, or external hard disks. Taxpayer data exchange for internal purposes must be authorized by the administrator or carried out directly, not by the tax authorities.

The biggest challenge in maintaining the security of taxpayer data is not on the internal aspect of the tax employee but the external aspect, in this case, the taxpayer himself, as the data owner who does not understand and tends to ignore the security aspect the taxpayer's E-Filing account. Often taxpayers use easy passwords for hackers to guess, such as date of birth, either the date of birth themselves or those closest to them. Then taxpayers also use standard and very commonly used passwords, such as abc, 123, abc123, 12345, a123, xyz, and other simple sentences that are very easy to guess. The previous leak was the taxpayer's negligence, who used an easy password for hackers to guess. Then the hacker entered the DGT website using the taxpayer's account that he had hijacked. The hackers tried to steal taxpayer data on the DGT server, but their efforts failed because they were blocked by a firewall installed on the DGT server. The hackers only got the passwords for several E-Filing accounts belonging to taxpayers, which did not have a significant impact because the data taxpayers could access was very limited. It is different if the hacker can break into the password of the taxpayer administrator who has full authority in managing taxpayer data in each KPP. Of course, the damage caused will be much more significant.

DGT often faces obstacles to securing taxpayer data on technical issues in each KPP. These server problems are often errors and cannot be accessed by tax authorities or taxpayers. Sometimes the server experiences an error during working hours so that the tax authorities cannot process tax reporting through E-filing carried out by taxpayers, or taxpayers themselves cannot report taxes through E-Filing. This condition occurs almost every day, and although it does not last long, it is felt to be quite disturbing to the smooth process of tax reporting by taxpayers and processing of reports by the tax authorities. For this reason, academics suggest that the DGT immediately upgrade the information system currently owned by the DGT so that the technical aspects can be minimized and do not interfere with the taxpayer reporting process. The Ministry of Finance should pay more attention to the hardware quality of the server used by the DGT, considering that the server stores data from hundreds of millions of taxpayers in Indonesia. Of

course, it will be detrimental to the national interest if the DGT server is damaged or loses priceless data.

Barriers from internal organizational aspects that often occur, for example, are human errors made by the tax authorities, for example, forgetting to log out after accessing taxpayer data, leaving taxpayer data open on the work desk, or losing data because it is accidentally deleted or formatted. Of course, the DGT will not tolerate a phenomenon like this because it can harm the DGT and the taxpayer. If the error occurs, a verbal warning will be given to the tax authorities concerned. If the error is repeated, a written warning will be given, and if the same error is repeated and is made intentionally, action will be taken in a dismissal sanction.

Table I. Target and Realization of Indonesia's Tax Revenue for the Year 2018-2021

Year	Target	Realization	Percentage
2018	1,424,00 T	1,315,51 T	92,24%
2019	1,315,51 T	1,332,06 T	84,44%
2020	1,198,82 T	1,070,00 T	89,3%
2021	1,229,6 T	1,231,87 T	100,19%

Source: Directorate General of Taxes Performance Report Year 2018-2021

Based on Table 1, Tax Revenue in Indonesia from 2018 to 2021 has increased and decreased in the presentation of revenue achievements. In 2019, there was a decrease in achievement of 84.44%, compared to 2018 of 92.24%. Meanwhile, from 2020 to 2021, the percentage increased. After getting the results, the researchers conducted data analysis and interpretation of the discussion of the data obtained as a result of research using the data analysis presented above. Based on the results of research on the Effectiveness of Taxpayer Data Security in Implementing Tax Obligations at the Directorate General of Taxes.

Effectiveness of Taxpayer Data Security in Implementing Tax Obligations at the Directorate General of Taxes

Effectiveness is a measure of the success or failure of an organization in achieving its goals, showing in terms of whether or not the goals that have been set have been achieved. In the digital era of electronic communication, a person can make transactions or communications quickly and easily. This condition affects significant developments in information technology. Where the internet is getting bigger with cheaper access costs, the consequence is that the risk in data and information security is increasing. Data security is the protection of data within a system against unauthorized authorization, modification, or destruction and the protection of computer systems against unauthorized use or modification. Now, even to log in to DGT, users cannot only log in. They have to join a domain because of the power of a country to ensure that tax data is not compromised.

Based on E-45/PJ/2020, it aims to guide provisions, mechanisms, and parties involved in securing devices and data and information processing facilities. This guideline requires all DGT employees to secure their computer equipment to prevent unwanted problems that will jeopardize data security and the integrity of information assets to disrupt DGT's activities. The policy that has been made requires outside parties or third parties who enter the DGT environment to wear an official identity card from the DGT. The procedures and provisions for securing data and information processing equipment and facilities are listed in attachment SE-45/PJ/2020. SE-16/PJ/2011. In Effectiveness of Taxpayer Data Security in Implementing Tax Obligations at the Directorate General of Taxes, the authors used the theory of Richard M Streed (Khaerul Umam: 2015).

Organizational Characteristics

Organizational characteristics are an arrangement of Human Resources to form an organization and affect the Effectiveness of Data Security in Implementing Tax Obligations. So that the people in this organization are experts, competent, and highly responsible.

Based on the interviews with informants regarding organizational characteristics in the effectiveness of taxpayer data security, there is a section tasked with securing taxpayer data so that there are no things that want to hack taxpayer data. Every employee is not allowed to receive unknown emails to avoid viruses from those emails that once caused a data leak. In addition, in maintaining the security of taxpayer data, the efforts made are to find human resources with certain criteria and have good integrity for that and advance all policies that have been prepared. Improving work systems or good programs so that hackers cannot access or find it difficult to steal taxpayer data becomes a big goal in protecting all taxpayer data.

Environmental Characteristics

Two aspects exist in environmental characteristics, namely, aspects of the internal and external environment. Aspects of the internal environment are those within the organization, while aspects of the external environment are entirely within the organization. Environmental characteristics are an important factor in maintaining the security of taxpayer data. Based on the information obtained by the authors from interviews with informants, environmental characteristics are related to the integrity and responsibility of employees in maintaining taxpayer data. The importance of confidentiality of a taxpayer's data or documents so that officers should not be negligent because such negligence can cause something undesirable.

Employee Characteristics

The characteristics of workers are important factors in effectiveness, in each individual will generally find many differences that greatly affect the goals of the organization, therefore must be able to integrate personal goals with organizational goals. Based on the interviews with informants, the characteristics of workers are by preparing and improving data security through the system and improving the quality of human resources in terms of quality, skills, and integrity.

Management Characteristics

Characteristics of management are a strategy and work mechanism used to regulate all aspects until the effectiveness of the plan or policy is achieved to achieve organizational goals. Based on the interviews with informants, management's characteristics are improving the system's quality and increasing human resources in terms of skills and integrity, as well as increasing data security and confidentiality from third parties who try to enter.

Obstacles in the Effectiveness of Taxpayer Data Security in Implementing Tax obligations at the Directorate General of Taxes

Based on the interviews, the obstacles that affect the effectiveness of data security of taxpayers in carrying out tax obligations at the Directorate General of Taxes. Among them are caused by the internet network that is not yet stable, human error, and punishment that is not strong enough.

Efforts in Effectiveness of Taxpayer Data Security in Implementing Tax obligations at the Directorate General of Taxes

The efforts to overcome the obstacles to the Effectiveness of Taxpayer Data Security in Implementing Tax Obligations at the Directorate General of Taxes are as follows: (1) Conducting regular training to improve the quality of officers; (2) Making regulations for employees who are negligent and violate the rules; (3) Educate taxpayers about the importance of data privacy of taxpayers; and (4) Running a work program that has been neatly arranged so that it runs perfectly and gives maximum results.

Comparison with the Effectiveness of Taxpayer Data Security in Other Countries

Russia

Through the built information system model, taxpayer data security in Russia considers the main directions of developing existing tax policies, evaluates the threat of taxpayer data leakage, and studies ideas and indicators of the quality of taxation data management in Russia. The

analysis of the tax information system will be used in the future strategic planning system of the Russian taxation system. In addition, the development and establishment of a tax data security strategy that allows further correction of the state tax collection system by using the methods and means applied to the tax collection system by collaborating with software developers to build a capable tax data security system.

By evaluating the level of security of taxpayer data in the information system, the Russian Federal Tax Service can implement information systems and digital services step by step into service activities for taxpayers. A transfer strategy makes it easier for taxpayers to make tax reporting. All policies to secure taxpayer data are prepared based on the main national target indicator in the field of taxation, namely the establishment of a Tax-Adjusted Information Society in 2020. The Strategic Plan and policy implementation by the Russian Federal Tax Service aim to reduce political interference in domestic tax management so that it can increase revenue from the tax sector and build a tax system that is effective, safe, and protected from external threats (Fedotova et al., 2019).

French

Through the adoption of the Internet of Things (IoT), the French State Tax Bureau is faced with a big challenge for the tax authorities. After several years of administrative reforms inspired by the New Public Management and New Public Governance, the State Tax Bureau is ready to adopt IoT-based solutions to improve the efficiency and effectiveness of public services, including tax services. The French government uses a theoretical approach in adopting this innovation of the Regional Tax Agency by integrating information technology systems resulting from reforms in the field of public administration. With the adoption of IoT technology, the complexity and risk of taxpayer data leakage have become small. Through tax administration reforms, tax authorities can adopt IoT technology to improve efficiency, service quality, and taxpayer participation. Suppose efficiency improvements in taxpayer data security can be achieved. In that case, public confidence in this new technology will help address concerns about the complexity of the technology and the potential for data leaks. (Leroux & Pupion, 2022).

China

Using the Consolidated State and Local Tax Bureau (CSLTB) policy in China to protect sensitive taxpayer data in the cloud computing environment, issues such as data ownership, data access control, transparency, and auditing of information systems arise. An access control mechanism system was created based on the blockchain system to overcome this problem. It is more efficient and effective because it does not require a lot of human resources and can increase the risk of leakage. The tax information system allows access control of taxpayer data based on blockchain. Data-related activities such as uploading, updating, and downloading can be processed automatically and ensure the transparency and accountability of the tax information system. The blockchain model satisfies all the taxpayer's data protection requirements and does not carry any additional security risks. In addition, the blockchain model is easier to use by taxpayers and tax authorities both from a computing perspective and a communication perspective (Yang et al., 2021).

CONCLUSION

Based on the results, discussion, and interpretation described in previous chapters and the theory and results of previous studies, it can be concluded as follows: (1) Effectiveness of Taxpayer Data Security in Implementing Tax Obligations at the Directorate General of Taxes. From the taxpayer data leak, the DGT ensures that the taxpayer's data is now guaranteed safe. Considering that the security of taxpayer data is vital and confidential, DGT makes several efforts to avoid attacks by hackers that cause taxpayer data to leak. The actions taken by the DGT justify; (2) Obstacles that affect the Effectiveness of Taxpayer Data Security in Implementing Tax Obligations at the Directorate General of Taxes are the lack of knowledge of taxpayers regarding the importance of maintaining data confidentiality, internet network instability, the number of people trying to hack into DGT data; (3) Efforts made to overcome obstacles that affect the

Effectiveness of Taxpayer Data Security in Implementing Tax Obligations are actively changing passwords periodically, conducting training for every employee in charge of maintaining the security of taxpayer data. Moreover, avoid receiving an email that is unknown because the email could carry a virus, which becomes a cause or a contributing factor to the leakage of taxpayer data.

Based on a comparison with taxpayer data security practices in 3 (three) countries, namely Russia, France, and China, Indonesia appears to be a bit behind in tax information system technology that stores data on hundreds of millions of taxpayers. Russia already has a strategic plan for a tax service information system known as the Tax-Compliant Information Society in 2020. Through the evaluation process of the level of security of taxpayer data in the information system, the Russian Federal Tax Service can implement information systems and digital services step by step into service activities against taxpayers. The Strategic Plan and policies of the Russian Federal Tax Service aim to reduce political interference in tax management in the country to increase revenue from the taxation sector and build an effective, safe, and protected tax system from external threats.

Meanwhile, in France, the government uses a theoretical approach in adopting Internet of Things technology innovation in the Regional Tax Agency by integrating information technology systems resulting from reforms in public administration. Adopting IoT technology makes the complexity and risk of taxpayer data leakage small. The tax authorities, through the implementation of tax administration reforms, can adopt IoT technology to improve efficiency, service quality, and taxpayer participation.

Furthermore, through the Consolidation of State and Local Tax Bureaus (CSLTB), the Chinese government already has a taxpayer data security system by adopting blockchain technology such as crypto-currencies like Ethereum. Data-related activities such as uploading, updating, and downloading can be processed automatically and ensure the transparency and accountability of the tax information system. The blockchain model satisfies all the taxpayer's data protection requirements and does not carry any additional security risks. In addition, the blockchain model is easier to use by taxpayers and tax authorities both from a computing perspective and a communication perspective. Based on the discussion and conclusions that have been stated above, the authors, therefore, propose the following for consideration: (1) Improving the security of taxpayer data so that its confidentiality is further maintained and carrying out innovations to strengthen the security of taxpayer data; and (2) Making efforts to make regulations made by the Directorate General of Taxes to parties who try to leak taxpayer data, both from external and internal office parties.

REFERENCES

Acharya, S., & Mekker, M. (2022). Public acceptance of connected vehicles: An extension of the technology acceptance model. *Transportation Research Part F: Traffic Psychology and Behaviour*, *88*, 54–68. https://doi.org/10.1016/j.trf.2022.05.002

Adi, I. K. Y. (2020). Efektifitas E–Filing Terhadap Peningkatan Kepatuhan Wajib Pajak Orang Pribadi dengan Tingkat Keamanan dan Kerahasiaan Sebagai Variabel Moderasi (Studi Empiris Pada Kantor Pelayanan Pajak Pratama Badung Utara). *Journal of Applied Management and Accounting Science*, *2*(1), 53–66. https://doi.org/10.51713/jamas.v2i1.26

Adi, K., Hamza, L., & Pene, L. (2018). Automatic security policy enforcement in computer systems. *Computers & Security*, *73*, 156–171. https://doi.org/10.1016/j.cose.2017.10.012

Al Hujran, O., Aloudat, A., & Altarawneh, I. (2013). Factors Influencing Citizen Adoption of E-Government in Developing Countries. *International Journal of Technology and Human Interaction*, *9*(2), 1–19. https://doi.org/10.4018/jthi.2013040101

Albram, D. (2016). Perspektif Kelembagaan Direktorat Jenderal Bea dan Cukai (DJBC) dalam Bidang Pelayanan Kemudahan Impor Tujuan Ekspor (KITE) Di Indonesia. *Jurnal Penelitian Hukum De Jure*, *16*(1), 105. https://doi.org/10.30641/dejure.2016.V16.105-118

Alnemer, H. A. (2022). Determinants of digital banking adoption in the Kingdom of Saudi Arabia: A technology acceptance model approach. *Digital Business*, 100037. https://doi.org/10.1016/j.digbus.2022.100037

Arikunto, S. (2013). *Prosedur Penelitian: Suatu Pendekatan Praktik* (8th ed.). Rineka Cipta. https://opac.perpusnas.go.id/DetailOpac.aspx?id=217760

Aziz, S. A., & Idris, K. M. (2014). Does Design Matter in Tax E-filing Acceptance? *Procedia - Social and Behavioral Sciences*, *164*, 451–457. https://doi.org/10.1016/j.sbspro.2014.11.102

Bag, P. K., & Wang, P. (2021). Income tax evasion and audits under common and idiosyncratic shocks. *Journal of Economic Behavior & Organization*, *184*, 99–116. https://doi.org/10.1016/j.jebo.2021.01.022

Bahri, S., & Listiorini, L. (2019). Pengaruh Persepsi Kegunaa, Persepsi Kemudahan, Persepsi Keamanan dan Kerahasiaan dan Persepsi Kecepatan Terhadap Minat Wajib Pajak dalam Menggunakan E-Filing pada KPP Pratama Binjai. *Jurnal Riset Akuntansi Dan Bisnis*, *19*(2), 159–170. https://doi.org/10.30596/jrab.v19i2.4680

Bel, G., Bel-Piñana, P., & Rosell, J. (2017). Myopic PPPs: Risk allocation and hidden liabilities for taxpayers and users. *Utilities Policy*, *48*, 147–156. https://doi.org/10.1016/j.jup.2017.06.002

Binder, B., & Haupt, A. (2022). The fundamental role of tax systems in the relationship between workfare and inequality in the lower half of the income distribution. *Research in Social Stratification and Mobility*, *80*, 100712. https://doi.org/10.1016/j.rssm.2022.100712

Butarbutar, R. (2017). *Hukum Pajak Indonesia dan Internasional* (O. D. Putri (ed.); 1st ed.). Gramata Publishing. https://opac.perpusnas.go.id/DetailOpac.aspx?id=1146222

Cappelletti, G., Guazzarotti, G., & Tommasino, P. (2017). The stock market effects of a securities transaction tax: Quasi-experimental evidence from Italy. *Journal of Financial Stability*, *31*, 81–92. https://doi.org/10.1016/j.jfs.2017.05.003

Castellón González, P., & Velásquez, J. D. (2013). Characterization and detection of taxpayers with false invoices using data mining techniques. *Expert Systems with Applications*, *40*(5), 1427–1436. https://doi.org/10.1016/j.eswa.2012.08.051

Chairani, H., & Farina, K. (2021). Pengaruh Persepsi Kebermanfaatan, Persepsi Kemudahan serta Keamanan dan Kerahasiaan Terhadap Penggunaan E-Filing Wajib Pajak UMKM. *JRAK: Jurnal Riset Akuntansi Dan Keuangan*, *7*(2), 71–84. https://doi.org/https://doi.org/10.38204/jrak.v7i2.545

Compaoré, A. (2022). Access-for-all to financial services: Non-resources tax revenue-harnessing opportunities in developing countries. *The Quarterly Review of Economics and Finance*, *85*, 236–245. https://doi.org/10.1016/j.qref.2022.03.007

Creswell, J. W. (2017). *Research Design Pendekatan Kualitatif, Kuantitatif, dan Mixed* (S. Z. Qudsy (ed.); 3rd ed.). Pustaka Pelajar. https://opac.perpusnas.go.id/DetailOpac.aspx?id=1213690

Dantes, H. P., & Lasminiasih. (2021). Analisis Tingkat Efektivitas dan Kontribusi Pajak Restoran Terhadap Pendapatan Asli Daerah di Provinsi DKI Jakarta Tahun 2017-2019. *Jurnal Inovasi Penelitian*, *1*(12), 2743–2750. https://doi.org/https://doi.org/10.47492/jip.v1i12.537

Detik Finance. (2022, March 3). DJP Buka Suara Soal Dugaan Data Wajib Pajak Bocor. *Detik.Com*, 1–3. https://finance.detik.com/berita-ekonomi-bisnis/d-5967346/djp-buka-suara-soal-dugaan-data-wajib-pajak-bocor

Dewi, M. A. C. (2019). Pengaruh Persepsi Kegunaan, Persepsi Kemudahan, Keamanan dan Kerahasiaan, Tingkat Kesiapan Teknologi Informasi dan Kepuasan Pengguna Wajib Pajak Terhadap Intensitas Perilaku Wajib Pajak Dalam Penggunaan E-Filing. *JSAM: Jurnal Sains Akuntansi Dan Manajemen*, *1*(3), 317–368. https://doi.org/https://doi.org/10.1234/jsam.v1i3.66

Dong, S. X., & Sinning, M. (2022). Trying to Make a Good First Impression: A Natural Field Experiment to Engage New Entrants to the Tax System. *Journal of Behavioral and Experimental Economics*, *100*, 101900. https://doi.org/10.1016/j.socec.2022.101900

Fang, H., Su, Y., & Lu, W. (2022). Tax incentive and corporate financial performance: Evidence from income tax revenue sharing reform in China. *Journal of Asian Economics*, *81*, 101505. https://doi.org/10.1016/j.asieco.2022.101505

Faúndez-Ugalde, A., Mellado-Silva, R., & Aldunate-Lizana, E. (2020). Use of artificial intelligence by tax administrations: An analysis regarding taxpayers' rights in Latin American countries. *Computer Law & Security Review*, *38*, 105441. https://doi.org/10.1016/j.clsr.2020.105441

Fazri, I. L. (2017). *Analisis Persepsi Kegunaan Dan Persepsi Keamanan Dan Kerahasian Terhadap Penggunaan E-Filling (Studi Kasus Pada Wajib Pajak Orang Pribadi di KPP Pratama Garut)* [UNIKOM]. https://repository.unikom.ac.id/54082/

Fedotova, G. V., Ilyasov, R. H., Gontar, A. A., & Ksenda, V. M. (2019). *The Strategy of Provision of Tax Security of the State in the Conditions of Information Economy* (pp. 217–228). https://doi.org/10.1007/978-3-030-01514-5_25

Feng, C., Ye, Y., & Tao, Y. (2022). Tax Authority Enforcement and Corporate Social Security Contributions: Evidence from China. *Finance Research Letters*, *49*, 103094. https://doi.org/10.1016/j.frl.2022.103094

Fernandes, D. A. B., Freire, M. M., Fazendeiro, P. A. P., & Inácio, P. R. M. (2017). Applications of artificial immune systems to computer security: A survey. *Journal of Information Security and Applications*, *35*, 138–159. https://doi.org/10.1016/j.jisa.2017.06.007

Fu, C., Xue, M., Xu, D.-L., & Yang, S.-L. (2019). Selecting strategic partner for tax information systems based on weight learning with belief structures. *International Journal of Approximate Reasoning*, *105*, 66–84. https://doi.org/10.1016/j.ijar.2018.11.009

Gavard, C., Voigt, S., & Genty, A. (2022). Using emissions trading schemes to reduce heterogeneous distortionary taxes: The case of recycling carbon auction revenues to support renewable energy. *Energy Policy*, *168*, 113133. https://doi.org/10.1016/j.enpol.2022.113133

Hapsari, M. T., Domai, T., & Hidayati, F. (2018). Penilaian Intensifikasi PBB P2 dalam Meningkatkan Penerimaan Daerah. *Jurnal Akuntansi Dan Pajak*, *19*(1), 21. https://doi.org/10.29040/jap.v19i1.197

Hifni, N. (2022, May 24). Regulasi Menjamin Keamanan Data Digital. *Majalah Pajak*, 1–5. https://majalahpajak.net/regulasi-menjamin-keamanan-data-digital/

Kariyoto, K. (2012). Pengaruh Kesadaran dan Kepatuhan Wajib Pajak Terhadap Kinerja Perpajakan. *Jurnal Akuntansi Multiparadigma*. https://doi.org/10.18202/jamal.2012.04.7145

Leroux, E., & Pupion, P.-C. (2022). Smart territories and IoT adoption by local authorities: A question of trust, efficiency, and relationship with the citizen-user-taxpayer. *Technological Forecasting and Social Change*, *174*, 121195. https://doi.org/10.1016/j.techfore.2021.121195

Lin, B., & Jia, Z. (2019). Tax rate, government revenue, and economic performance: A perspective of Laffer curve. *China Economic Review*, *56*, 101307. https://doi.org/10.1016/j.chieco.2019.101307

Liu, J., Luo, X., Liu, X., Li, N., Xing, M., Gao, Y., & Liu, Y. (2022). Rural residents' acceptance of clean heating: An extended technology acceptance model considering rural residents' livelihood capital and perception of clean heating. *Energy and Buildings*, *267*, 112154. https://doi.org/10.1016/j.enbuild.2022.112154

Low, S., Ullah, F., Shirowzhan, S., Sepasgozar, S. M. E., & Lin Lee, C. (2020). Smart Digital Marketing Capabilities for Sustainable Property Development: A Case of Malaysia. *Sustainability*, *12*(13), 5402. https://doi.org/10.3390/su12135402

Marlina, L., & Syahribulan, S. (2021). Peranan Insentif Pajak Yang Di Tanggung Pemerintah (DTP) Di Era Pandemi Covid 19. *Economy Deposit Journal (E-DJ)*, *2*(2). https://doi.org/10.36090/e-dj.v2i2.910

Matti, S., Nässén, J., & Larsson, J. (2022). Are fee-and-dividend schemes the savior of environmental taxation? Analyses of how different revenue use alternatives affect public support for Sweden's air passenger tax. *Environmental Science & Policy*, *132*, 181–189. https://doi.org/10.1016/j.envsci.2022.02.024

Megayani, N. K. M., & Noviari, N. (2021). Pengaruh Program E-SAMSAT, SAMSAT Keliling, dan Kepuasan Wajib Pajak pada Kepatuhan Wajib Pajak Kendaraan Bermotor. *E-Jurnal Akuntansi*, *31*(8), 1936. https://doi.org/10.24843/EJA.2021.v31.i08.p05

Moleong, J. L. (2018). *Qualitative Research Methodology*. Rosdakarya Youth.

Ndoricimpa, A. (2021). Tax reforms, civil conflicts, and tax revenue performance in Burundi. *Scientific African*, *13*, e00927. https://doi.org/10.1016/j.sciaf.2021.e00927

Norzhela, B., Rauf, S. A., & Hermawansyah, A. (2019). Analisis Efektivitas Kepuasan Wajib Pajak

Dalam Pengisian Laporan SPT DJP Online. *J-Sim : Jurnal Sistem Informasi*, *2*(2), 55–59. http://ojs.stmik-borneo.ac.id/index.php/J-SIm/article/view/50

Pohan, C. A. (2021). *Kebijakan dan Administrasi Perpajakan Daerah di Indonesia* (1st ed.). Gramedia Pustaka Utama. https://ebooks.gramedia.com/id/buku/kebijakan-dan-administrasi-perpajakan-daerah-di-indonesia

Purnomo, B. (2022, March 4). Dirjen Pajak Tanggapi Isu Mengenai Kebocoran Data 49 Ribu Credential Wajib Pajak. *Hallo.Id*, 1–5. https://www.hallo.id/ekonomi-bisnis/pr-282841059/dirjen-pajak-tanggapi-isu-mengenai-kebocoran-data-49-ribucredential-wajib-pajak

Rafique, H., Almagrabi, A. O., Shamim, A., Anwar, F., & Bashir, A. K. (2020). Investigating the Acceptance of Mobile Library Applications with an Extended Technology Acceptance Model (TAM). *Computers & Education*, *145*, 103732. https://doi.org/10.1016/j.compedu.2019.103732

Ratnawati, D. (2016). Carbon Tax Sebagai Alternatif Kebijakan Untuk Mengatasi Eksternalitas Negatif Emisi Karbon di Indonesia. *Indonesian Treasury Review Jurnal Perbendaharaan Keuangan Negara Dan Kebijakan Publik*, *1*(2), 53–67. https://doi.org/10.33105/itrev.v1i2.51

Reck, D., Slemrod, J., & Vattø, T. E. (2022). Public disclosure of tax information: Compliance tool or social network? *Journal of Public Economics*, *212*, 104708. https://doi.org/10.1016/j.jpubeco.2022.104708

Said, A. A. (2022, March 4). DJP Pastikan Data Wajib Pajak Aman Meski Terjadi Kebocoran. *Katadata.Co.Id*, 1–3. https://katadata.co.id/happyfajrian/finansial/6221714958e08/djp-pastikan-data-wajib-pajak-aman-meski-terjadi-kebocoran

Samudra, A. A. (2016). *Perpajakan di indonesia: Keuangan, Pajak dan Retribusi Daerah* (2nd ed.). PT Rajagrafindo Persada. https://opac.perpusnas.go.id/DetailOpac.aspx?id=928594

Santoro, F. (2021). To file or not to file? Another dimension of tax compliance - the Eswatini Taxpayers' survey. *Journal of Behavioral and Experimental Economics*, *95*, 101760. https://doi.org/10.1016/j.socec.2021.101760

Scherer, R., Siddiq, F., & Tondeur, J. (2019). The technology acceptance model (TAM): A meta-analytic structural equation modeling approach to explaining teachers' adoption of digital technology in education. *Computers & Education*, *128*, 13–35. https://doi.org/10.1016/j.compedu.2018.09.009

Setiawan, D. A. (2021, August 24). Cegah Data Wajib Pajak Disalahgunakan, DJP Lakukan Langkah Ini. *DDTC News*, 1–5. https://news.ddtc.co.id/cegah-data-wajib-pajak-disalahgunakan-djp-lakukan-langkah-ini-32226

Setiowati, Y. D., Fauzi, A., & Sumiati, A. (2020). Pengaruh Kepatuhan Wajib Pajak Perusahaan dan Audit Pajak Terhadap Pendapatan Pajak Penghasilan Perusahaan : Studi Kasus di Kantor Pelayanan Pajak Jakarta Kebayoran Lama. *Jurnal Bisnis Manajemen Dan Keuangan*, *1*(2), 407–415. http://pub.unj.ac.id/index.php/jbmk/article/view/114/133

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI*, *27*(1), 38. https://doi.org/10.47268/sasi.v27i1.394

Sugiyono. (2019). *Metode Penelitian Kuantitatif Kualitatif dan R&D* (I). Alfabeta. https://cvalfabeta.com/product/metode-penelitian-kuantitatif-kualitatif-dan-rd-mpkk/

Wardani, D. K., Putry, N. A. C., & Dewi, F. A. K. (2021). Pengaruh Persepsi Keamanan dan Kerahasiaan Terhadap Niat Membayar Pajak Menggunakan Pajakpay. *AKURAT: Jurnal Ilmiah Akuntansi*, *12*(1), 108–116. https://ejournal.unibba.ac.id/index.php/akurat/article/view/394

Wiczorek, R., & Zirk, A. (2019). Using warning systems with adaptable thresholds: Choice of security level, compliance, and performance in a simulated computer security task. *International Journal of Human-Computer Studies*, *125*, 32–40. https://doi.org/10.1016/j.ijhcs.2018.12.006

Wulandari, D. S. (2021). Digitalisasi Sistem Administrasi Perpajakan dan Biaya Kepatuhan Pajak Terhadap Kepatuhan Wajib Pajak Orang Pribadi. *Journal of Accounting Science*, *5*(1), 36–70. https://jas.umsida.ac.id/index.php/jas/article/view/1131

Xiao, C., & Shao, Y. (2020). Information system and corporate income tax enforcement: Evidence from China. *Journal of Accounting and Public Policy*, *39*(6), 106772. https://doi.org/10.1016/j.jaccpubpol.2020.106772

Yang, Z., Chen, Y., Huang, Y., & Li, X. (2021). *Protecting personal sensitive data security in the cloud with blockchain* (pp. 195–231). https://doi.org/10.1016/bs.adcom.2020.09.004