

# Application of Authentication in Peer to Peer Lending Fintech Transactions to Maintain the Confidentiality of Personal Data

Fery Suryono<sup>1</sup>, Rineke Sara<sup>2</sup>  
{Feryfelis@gmail.com<sup>1</sup>, rineke\_sara@borobudur.ac.id<sup>2</sup>}

Universitas Borobudur, Jakarta, Indonesia<sup>1,2</sup>

**Abstract.** This exploration is roused by the development of numerous issues from Fintech Peer to Peer Lending administrations. Fintech Peer to Peer Lending administration is an advance and acquiring administration in rupiah money straightforwardly between banks/moneylenders (banks) and account holders/borrowers (credit beneficiaries) in view of data innovation. Fintech Peer to Peer Lending likewise gives offices to support proprietors to offer credits straightforwardly to indebted individuals with more significant yields. Interestingly, store borrowers can apply for credit presently to support proprietors with more direct terms and a quicker interaction than ordinary monetary foundations. The strategy utilized in this exploration is regularizing juridical with a writing concentrate on approach. The results obtained from this study are the problems that arise from P2P lending fintech activities, including personal information that is easily disclosed, resulting in the leakage of personal data of lenders and borrowers.

**Keywords:** Fintech; P2P Lending; Personal Data

## 1 Introduction

Indonesia is an archipelagic country with the most population in Asia. It has more than 260 million people spread across 17,000 islands and spreads from west to east and north to south.[1] The form of an archipelagic state like that makes the Indonesian government experience several obstacles in providing its services.[2] One of the forms of service constraints is the distribution of banking services in Indonesia in carrying out their duties to improve the people's standard of living. Because it is believed that it will support poverty reduction programs and reduce the gap in the community's economic capacity, this happens because of Indonesia's geographical location, which is an archipelagic country. Public outreach to banking services becomes difficult because banking itself is not evenly distributed. Banking services are only piled up in the city center, not touching people in remote areas. In conclusion, this problem causes the welfare gap in Indonesia due to the uneven development of the national economy.[3]

The business there is run in banking activities is a complete risk business because its activation primarily relies on funds deposited by the public. Strong regulations must support

the significant role of banks in economic activities.[4] There is an effort to realize healthy banking. But along with the development of the times in this era of globalization, any community activity will not be separated from the help of technology. Likewise, financial institutions are now starting to shift to technology-based financial institutions. One of the advancements in the financial sector today is the adaptation of financial technology.[5]

Fintech itself is a startup that is starting to rise in the current era. The concept adopted by fintech is a combination of finance and technology combined with modern innovation. It is hoped that this can make the process of financial transactions more practical and safe to use. The essential types of fintech incorporate installments (computerized wallets, P2P installments), venture (value crowdfunding, Peer to Peer Lending), financing (crowdfunding, miniature advances, credit offices), Insurance (hazard the executives), Cross-process (broad information examination, prescient demonstrating), foundation (security).[6] The development of fintech has brought about monetary organizations, one of which is data innovation based loaning and getting administrations (shared or P2P loaning).[3]

The expanding number of fintech organizations showing up in the field (distributed or P2P loaning) is without a doubt getting the public's consideration and the public authority, for this situation, the controller, in particular the Financial Services Authority (OJK), and Bank Indonesia. There is expressed in the Financial Services Authority Regulation Number 77/POJK.01/2016 concerning Information Technology-Based Borrowing-Lending Services.

Peer-to-peer lending generally provides convenience to any party who wants to borrow funds or business capital. However, peer-to-peer lending is not always profitable for those who wish to borrow funds or money in practice. In an electronic contract or electronic agreement that should benefit both parties, it is even more inclined to the party who has total power in making the contract because the implementation of the peer-to-peer lending agreement is formed by default by the service provider of peer-to-peer lending. Because of this, the desired expectations in peer-to-peer lending services cannot be fully realized.[7]

However, it is necessary to understand that there must be an impact or obstacle in every facility, as in the case of online loans on peer-to-peer lending services. In this loan, all people can access it through an application downloaded on their respective smartphones. Being accessed through the application downloaded on each smartphone provides convenience that is very much different from conventional loans in general. The following way is to register, including your identity, and write an account number on online loans that are accessed through the application after the download process has been completed. Then the loan funds will immediately be disbursed.[8]

There are many cases of peer-to-peer lending services that often harm consumers due to agreements that favor the contract makers. Such as a lot of intimidation, terror, and law violations (sexual harassment, data dissemination, and others). These violations are the result of the Borrower not being able to pay off his debts. There is usually fintech which is generally not registered with the Financial Services Authority or can be said to be illegal fintech. In practice, online debt collectors often carry out these actions as parties who collect and notify payment due dates. Currently, many cases circulating reveal that this online loan application has a fatal impact, as indicated in the news in the media such as Kompas.com, which stated that there were many allegations of breaches of leaking personal data to sexual harassment—also circulating about this fintech violation case which was also quoted in tirto.id regarding a violation case of an application that terrorized debtors with personal data. It is true that after registering with personal identity and including an account number, the funds will immediately be disbursed. However, more than that, many people complain about the uncertain interest in the nominal range that must be paid when the payment period is due and

will increase when the debtor cannot pay it off. Also, when the debtor is unable to pay the debt, they will receive terrors from online debt collectors in the form of threats to the disclosure of personal identity.

Although in OJK Regulation No. 77/POJK.01/2016, as the regulatory authority in providing legal protection for online loans, this regulation has not protected the public. So if this can harm the community, it tends to be compared to honey or toxic substance, lawful fintech can measure up to cherish, and unlawful fintech is similar to a poison. Both run at the same time, offering on the web advances to people in general. Nonetheless, the last determinant is simply individuals who partake in the assistance, regardless of whether they need to drink honey or toxic substance.

Therefore, to prevent the spread of personal data by irresponsible persons, the manager of the P2P Lending application must provide authentication and security on the application before lenders or money borrowers transact through the application. With double authentication and security, of course, people can calmly use the application. It can legally be accounted for because it has a robust data security side that other parties outside the application manager do not easily hack.

## **2 Methods**

The type of research used is library research, namely research that utilizes secondary data. The source of the data can be obtained through document search. The author uses this research because before determining the type of research, the author first observes several places that match the title that has been taken. However, after watching the appropriate sites and the parties interviewed, research sources cannot be asked for information.

In writing this paper, the writer uses a normative research approach. The normative system is research that examines or analyzes secondary data, which can be in the form of secondary legal materials by understanding the law as a set of regulations or positive norms contained in the system of rules and regulations that apply in general. The researcher uses a normative approach because what the author will research and analyze are legal problems and legal remedies in using financial technology.

The data analysis method used in this research is qualitative analysis, which is a discussion carried out by combining library research and field research and interpreting and discussing primary data that has been obtained and processed as a whole. The results obtained from this analysis produce data referred to as descriptive data, namely data obtained from connecting data with one another, adjusted to the subject matter studied to become a unified whole.

## **3 Discussion**

### **3.1 Legal Problems in the Use of Financial Technology**

The emergence and birth of financial technology in Indonesia were born and developed due to people's lifestyles.[9] The Indonesian people, who usually transact face-to-face, began to shift to transact in a non-face-to-face or indirect manner. The existence of fintech in Indonesia has or has a beneficial impact on society, and this is because fintech provides convenience to every user when transacting electronically. One of the fintech currently widely used by the Indonesian people is the type of fintech peer-to-peer lending.[10] This type of

fintech is a company that provides financial services to bring together lenders and loan recipients to enter into lending and borrowing agreements in rupiah currency directly with an electronic system and using the internet network. The use of fintech peer-to-peer lending itself is so young. By downloading the fintech application and following the instructions in the application, people can interact easily without the need to go or visit the bank to borrow capital.

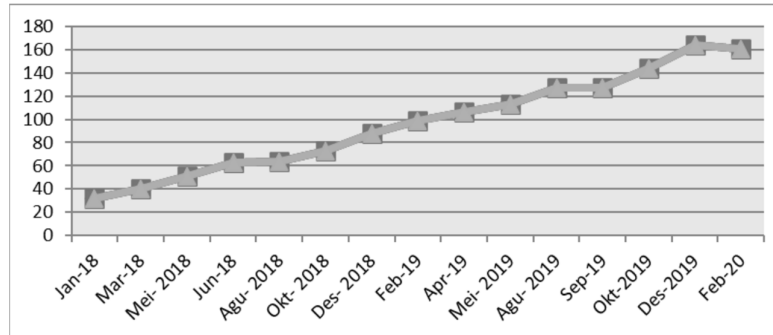


Fig. 1. The growth of fintech peer to peer lending companies in Indonesia

From the results of the author's research online, traditional loans, which are usually done directly by coming to the bank, with procedures that are so complicated and take a long time to make these loans are starting to be abandoned by the public and switch to fintech peer to peer lending. The peer-to-peer lending fintech company itself is a form of digitalization of established financial service companies, most notably collecting and distributing capital loans to the public. As of February 2020, there have been 161 operating fintech peer to peer lending companies in Indonesia. The rapid growth and development of this company in Indonesia are evident from the growth chart of fintech peer to peer lending below:

From the graph, it can be seen that starting from January 2018, when the Financial Services Authority began to open acceptance of registrations for fintech peer to peer lending until February 2020, there has been an increase where now the number of registered fintech peer to peer lending companies in Indonesia has reached 161 companies. From this graph, it can also be concluded that the increasing number of these companies proves that consumers of fintech distributed loaning in Indonesia are additionally expanding in number or can be supposed to be expanding in number. The bank is any individual, lawful substance, or business element with receivables because of a data innovation based loaning and acquiring administration contract. The meaning of a moneylender is contained in Article 1 point 8 of POJK No. 77/POJK.01/2016 concerning Information Technology-Based Lending and Borrowing Services. In the mean time, the meaning of borrowers and suppliers of data innovation based loaning and acquiring administrations is in Article 1 focuses 6 and 7 of POJK No. 77/POJK.01/2016 concerning Information Technology-Based Lending and Borrowing Services which reads as follows:

Data Technology-Based Lending and Borrowing Service Providers are Indonesian legitimate substances that give, oversee and work Information Technology-Based Borrowing-Lending Services. In the mean time, the Borrower is an individual or legitimate element with obligation because of an Information Technology-Based Borrowing and Borrowing Service arrangement. Recorded as a hard copy this paper, the coordinators and beneficiaries of Information Technology-Based Lending and Borrowing Services are purchasers and fintech

distributed loaning organizations. Coming up next is the relationship plan of the gatherings in the fintech shared loaning administration:

The scheme illustrates that the Peer to Peer Lending Fintech Service only consists of three parties: the Fintech Peer to Peer Lending Service provider, the lender, and the consumer/recipient of the Fintech Peer to Peer Lending Service. From the scheme above, the author can describe that the lender's function is to prepare loans that the Fintech Peer will distribute to Peer Lending Service providers to consumers or recipients of Fintech Peer to Peer Lending services. From this function, the author can also describe that the Fintech Peer to Peer Lending Service provider is a third party who acts as an intermediary in bringing together loan recipients and lenders using an electronic system. Meanwhile, recipients of services/consumers of Peer to Peer Lending Fintech Services are parties who have the position of seeking loans to meet their daily needs.

The Financial Services Authority recorded that the total number of lenders until February 2020 was 630,003 people, and the total number of loan recipients until February 2020 was 22,327,795 people. Therefore, if calculated, the total number of recipients or consumers of Peer Peer Lending fintech services in Indonesia as of February 2020 is 22,957,798 people. Meanwhile, the accumulated amount of loan distribution until February 2020 was IDR 95,394 57 billion.

Consumers of Peer Peer Lending fintech services are increasingly providing an excellent stimulus to Indonesia's economic growth. Micro, Small, and Medium Enterprises or MSMEs are some consumers who have received the most positive impacts from this Peer Lending fintech service. It was easier for them to find capital to develop their business with this service. It should be understood that if economic growth gets a positive stimulus and increases, it will automatically accelerate the national development of the State of Indonesia.

However, due to the outbreak of Covid-19, Fintech Peer to Peer Lending consumers in Indonesia are affected. These consumers cannot work, so they cannot earn income. A situation like today will cause the Borrower to be unable to pay the installments to default. For lenders, they cannot get back the funds lent through Fintech Peer to Peer Lending. If this situation continues, then consumers of peer-to-peer fintech loans in Indonesia will face severe problems due to the spread of Covid-19.

Conclusion: there is a means that 22,957,798 people will face these problems because Indonesia currently has 22,957,798 Fintech Peer to Peer Lending consumers. Situations like this require responsive laws/laws so that peer-to-peer financial technology fintech consumers can get legal protection. The responsive law must refer to laws that can answer all the problems faced by the community. Responsive law is a facilitator of various social needs and wants. Due to the outbreak of Covid-19, the difficulties faced by Fintech Peer To Peer Lending Consumers require legal protection that must be achieved through responsive legal development. This policy is essential because, with the outbreak of Covid-19 in Indonesia, there is a legal vacuum in consumer protection for Fintech Peer Peer Lending.

The legal vacuum in the perspective of positive law is the same as the vacuum of laws and regulations, or a rule or regulation made by the legislature to provide legal protection to the community. The emptiness or absence of the law in question is the absence of policies or rules from the government that protect consumers of peer-to-peer lending fintech services due to the spread of COVID-19 in Indonesia. Although there have been government regulations to stimulate credit relaxation for fintech peer-to-peer lending consumers, consumers do not feel a beneficial impact for consumers. The policy is OJK Regulation (POJK) Number 11/POJK.03/2020 concerning National Economic Stimulus as a Countercyclical Policy for the Impact of the 2019 Coronavirus Disease Spread.

In addition to legal problems caused by the covid-19 pandemic, recently there have also been many other problems related to fintech peer to peer lending services, as follows:

**a) The Rise of Illegal Peer to Peer Lending Fintech Services**

Each distributed loaning fintech supplier should be enrolled and acquire a license from the Financial Services Authority. There is plainly expressed in the Financial Services Authority Regulation Number 77 of 2016 concerning Information Technology-Based Lending and Borrowing Services Articles 7 and 8 so that if the organization doesn't have a grant and isn't enlisted with the Financial Services Authority, the organization is a fintech distributed loaning supplier. Unlawful. Through internet based exploration, the creator found undeniably more unlawful distributed loaning fintech organizations than those that have been enrolled. Proof from the Investment Alert Task Force has halted approximately 404 unlawful shared loaning fintech working in Indonesia.

In contrast, the number of licensed fintech peer-to-peer lending providers is only 78 companies. It should be understood that there is an apparent difference between companies providing fintech peer-to-peer lending and companies providing illegal peer-to-peer lending fintech. There can be seen in terms of the supervision of the protection offered by the companies giving fintech peer-to-peer lending will be more stringent if the company is a company that has been licensed.

So that if at any time there is a dispute between the fintech peer-to-peer lending company and the consumer/recipient of the fintech peer-to-peer lending service, then there will be regulations that mediate between them. Weak consumer protection for fintech peer-to-peer lending companies makes the company arbitrarily/violates its consumers, such as theft of personal data, intimidating billing, and the determination of high loan interest rates.

**b) The Number of Intimidating Billing to Consumers of Fintech Peer to Peer Lending Services**

This violation or problem is the problem that is most highlighted by the community. Here the company will take acts of offenses that lead to a form of intimidation, such as collecting arrears from customers who are past due with harsh words and threats of violence. This violation is not only carried out by illegal peer to peer fintech organizers, but even licensed companies often commit it. The author finds data that the company uses the desk collection party or a third party in the billing process in carrying out the billing.

Billing that is carried out in an intimidating manner is an act that is forbidden to be carried out by fintech peer-to-peer lending service providers. The prohibition is contained in the Code of Conduct of the Indonesian Fintech Association. It is evident in this provision that in terms of collecting loans to customers/consumers, the company must use good faith. The code of ethics also explains that the provider of peer-to-peer lending fintech services must have and notify the way of settlement and collection to consumers, namely the lender and the loan recipient, in the event of loan default.

The billing method or process consists of the company initially had to provide a warning letter to the recipient of the fintech peer to peer lending service, then the loan scheduling requirements, correspondence with the consumer of the fintech peer to examine lending service remotely, either via SMS, email and telephone. After that, the organizer is obliged to notify the consumer of the schedule of visits or communication with the collection team to cancel the loan. The code of ethics also implicitly explains that third parties in the billing

process are not included in the denylist of authorities. The meaning here is a certified third party.

#### **c) Determination Of High Loan Interest Rates**

High advance financing costs are remembered for a progression of issues in the fintech distributed loaning industry. The start of the fintech shared loaning industry is relied upon to give lower credit financing costs. In any case, the fintech business charges higher loan costs than banks and money organizations. The OJK has expressed that the financing cost for lawful fintech organizations' credits has arrived at 19% each month. In the interim, the financing costs for illicit fintech organizations are over the business normal. This deceptive fintech organization offers revenue that can be 2-3 percent each day.

#### **d) Misuse of Consumers' Data**

The vulnerability of misuse of personal data of fintech customers also continues to be a problem at this time. Current technological sophistication allows fintech companies to access personal data such as phone history and contact lists on mobile phones or smartphones, receiving fintech peer-to-peer lending services. Thus, fintech companies can find out the customer's personal profile without meeting in person by accessing this data. Accessing personal data for billing is a new thing for the general public. Most consumers of peer-to-peer lending fintech services often do not know that the terms of service or terms of condition allow fintech companies to access the data. In fact, by agreeing to the terms, personal data on consumer smartphones of fintech peer-to-peer lending services can be accessed by fintech providers. The use of customer personal data is one of the risks consumers must face when using fintech services. Billing with personal information is considered normal because it allows fintech companies to collect loans from their customers. Usually, fintech companies require an emergency contact so that it can be used for billing. In addition, by agreeing to the terms of service or condition before borrowing, the customer is deemed to have agreed to the fintech company accessing the personal data.

So from the four problems of implementing fintech here, the author can conclude that there is less than maximum supervision from the Financial Services Authority to ensure consumer security in the financial sector, especially consumers who use fintech services.

### **3.2 Implementation of Personal Data security by P2P Lending Operators in Indonesia**

The Operator must implement an information security management system to ensure the confidentiality and security of the P2P Lending Application User's Personal Data. This data confidentiality relates to the conception of privacy, which in practice relates to specific individual data. In contrast, data security (Data Security) relates to the efforts made by P2P Lending Operators in applying the principles of protection of Personal Data using a technology approach and business practices. That supports it. Based on POJK No. 77, one of the basic principles for protecting Application Users are data confidentiality and security. The privacy and security of this Personal Data are interrelated, where the confidentiality of data is highly dependent on the level of data security. The relationship between security and data privacy has always been complicated, and privacy depends absolutely on security.

Protection is the right of people to decide if Personal Data will be conveyed or not to different gatherings. In the utilization of data innovation, the assurance of Personal Data is one

piece of individual freedoms (security privileges). Individual privileges contain the accompanying implications: (a) the option to partake in a private life and be liberated from a wide range of obstruction, (b) the option to have the option to speak with others without spying, and (c) the option to screen admittance to data about an individual's very own life and information.

The security reasons should be ensured. In the first place, in building associations with individuals, an individual should cover a portion of his own life to keep up with his situation at a specific level. Second, somebody in his life needs an ideal opportunity to be separated from everyone else (isolation) so somebody needs security. Third, protection is a right that remains solitary and doesn't rely upon different freedoms, however this right will be lost if somebody distributes private things to the general population. Fourth, protection additionally incorporates an individual's on the whole correct to have homegrown relations, including how somebody fabricates a marriage, cultivates his family, and others may not know about this individual relationship, so Warren later considered it the right against the word. Fifth, another motivation behind why security merits lawful insurance is that the misfortunes endured are trying to evaluate. The misfortune is felt to be a lot more prominent than the actual misfortune since it has meddled with his own life so that in case there is a misfortune, the casualty should get pay.

Alan Westin first developed modern privacy theory in his book *Privacy and Freedom* who contends that security is the case of people, gatherings, or organizations to decide when, how, and how much data about them is imparted to other people. Put forward by Westin, then developed by other legal experts, especially in addressing the development and progress of information and communication technology. Westin has divided privacy into 4 (four) types: Solitude, Intimacy, Anonymity, and Reserve.

When associated with Application User Personal Data, all of the privacy categories above can be analyzed one by one. First, the P2P Lending Operator stores Application User financial data regarding the loan amount, loan status (paid off or in default), and loan maturity. According to the Personal Data Protection Bill (RUU PDP updated December 2019), financial data is included in Personal Data of a specific nature. Second, the P2P Lending Operator stores data on the Application User's body in the form of facial photos attached to other Personal Data such as hair type, which can be straight, curly, curly, rough, smooth, or bald; the shape of the face can be oval, oval or square; eye shape can be round, slanted, eye up, eye down; the shape of the cheekbones; The shape of the lips can be thick, thin, top thick, bottom narrow or vice versa, full thin and bottom wide. Application users who have uploaded photos of their faces into the P2P Lending application, there is a recording of Personal Data which is of course very dangerous if misused by the P2P Lending Operator, especially when it is entered into the Operator's electronic framework, the information proprietor no longer has a lot of command over the information. Once went into any IT framework like government's or corporate data set, individual data is at this point not in severe control of its proprietor. Application User's Personal Data put away in an electronic framework is a Digital Object attached to Material Rights, where each use of such data must follow a specific purpose. The data owner's consent must not be misused for purposes other than the agreed purpose.

One example of potential violations of data misuse is in the thee-KTP program, which requires a single identity of residents to be valid for life. Data recording includes citizens' personal information, including the person's physical characteristics, scanning fingerprints, and retinas of the eye, which are used for biometric validation of KTP holders. The problem point related to e-KTP is that the thee-KTP data storage server belongs to another country, so the data bank collected is very vulnerable to being accessed by foreign parties and is not

responsible. In P2P Lending, regarding servers, the Ministry of Communication and Information of the Republic of Indonesia requires that every P2P Lending Provider must have a server located in Indonesia to obtain a PSE Certificate. OJK also requires the same thing that P2P Lending Operators are required to use data centers and disaster recovery centers located in Indonesia. There is so that the data is not misused by other parties and brings losses to the owner of the Personal Data.

Third, the P2P Lending Manager saves conversation data with Application Users, for example, conversation data during the collection process for defaulted loans. Fourth, the P2P Lending Manager Application User data in the ID card, namely name, place of birth date, address, religion, marital, and employment status (includes Personal Data of a general nature). Loan recipients who fail to make payments are often visited by debt collectors in their homes and are intimidated using unlawful means. It is not legally allowed. Law No. 39 of 1999 concerning Human Rights (UU HAM), Article 31 stipulates that a person's residence may not be disturbed, stepped on or entered a yard of a home or entered a house contrary to the will of the person who inhabits it, only permitted in cases that have been determined by law. Personal Data as described in the 4 (four) categories above is stored in digital form in the form of electronic information or electronic documents in an electronic system and kept confidential as one of the obligations that the P2P Lending Operator must fulfill based on Article 26 paragraph (1) of PP PSTE. In addition, regarding the implementation of data confidentiality, based on POJK No. 77, P2P Lending Operators are required to:

- a. Maintain the classification, Integrity, and Availability of individual information, exchange information, and monetary information that it oversees from the time the information is gotten until the data is annihilated;
- b. Ensuring the Availability of confirmation, check, and approval processes that help disavowal in getting to, handling, and executing individual information, exchange information, and monetary information it oversees;
- c. Guarantee that the securing, use, usage, and revelation of individual information, exchange information, and monetary information got by the Operator depends on the endorsement of the proprietor of individual information, exchange information, and monetary information, except if in any case specified by the arrangements of laws and guidelines;
- d. Provide other correspondence media other than the Electronic System of Information Technology-Based Lending and Borrowing Services to guarantee coherence of client assistance, which can be as electronic mail, call focuses, or other correspondence media; and
- e. Notify the proprietor of the individual information, exchange information, and monetary information recorded as a hard copy in case of an inability to secure the classification of individual information, exchange information, and monetary information oversight by him.

P2P Lending Operators as Electronic System Operators should apply the ISO/IEC 27001 norm and the security arrangements specified by the Sector Supervisory and Regulatory Agencies. This ISO/IEC 27001 is a global standard arranged as a model for setting up, carrying out, working, checking, investigating, keeping up with, and further developing the Information Security Management System. The use of this ISO/IEC 27001 standard guarantees the assurance of Personal Data of Borrowers (Application Users) to accomplish data security, to be specific keeping up with classification, Integrity, and Availability of data.

Each P2P Lending Operator enrolled with the OJK, as well as being needed to get a PSE Certificate from the Ministry of Communication and Information, is likewise expected to acquire ISO/IEC 27001 affirmation to pass the permitting stage. There was expressed unequivocally when OJK gave a Registered Certificate to each P2P Lending Operator by

alluding to the arrangements of Article 28 section (2) of the Minister of Communication and Information Technology No. 4 of 2016, in particular "when this Ministerial Regulation comes into power, Electronic System Operators whose Electronic Systems have recently begun working should be confirmed for Information Security Management Systems no later than 1 (one) year after the Electronic Systems work".

The author analyzes that the ISO/IEC 27001 standard is part of the application of Privacy by Design, which is a theory that focuses on technological approaches and business practices to regulate privacy data. Personal Data Protection is not enough through legislation. Still, it must also be followed by information technology systems and business practices of P2P Lending Providers that always protect and pay attention to the rights of Application Users and supporting infrastructure, so that P2P Lending Providers can be trusted as a secure application platform in processing Personal Data. People need dependable practices all through the environment, which reaches out past ensuring protection to include information security, information precision, the reason for which information are utilized, and any "code of morals" that decides "proper" employments. For Privacy by Design to be carried out adequately, it should utilize the Basic Principles, in particular:

- a. Proactive, meaning that all tools, facilities, infrastructure, business practices must be prepared to protect data before losses occur.
- b. Default Settings, meaning that the system and infrastructure must be automatically created to protect data.
- c. Design-embedded means that data protection is provided in the IT design and company policies and business practices.
- d. Transparency, namely the disclosure of information to all users about the system and business practices used.
- e. End-to-end security, Privacy by Design that has been inserted into the framework before the main component of data is gathered, traversing the whole lifecycle of the information in question, beginning to end. This guarantees that all information is securely obliterated toward the finish of the cycle on schedule.
- f. Visibility and Transparency-Keep it Open, Privacy by Design which looks to guarantee all gatherings that any strategic policies or innovation included satisfy the guarantees and expressed objectives. Parts and tasks stay noticeable and straightforward.
- g. Respect Users, namely respecting users by always providing information about the privacy policy and making it easy for users to understand it.

Individual Data Security is one of the standards directed in the Personal Data Controller Bill (P2P Lending Providers remembered for it) are needed to secure and guarantee the security of the Personal Data they oversee, including the readiness and execution of functional, specialized strides to shield Personal Data from obstruction with the handling of Personal Data that is in opposition to arrangements of laws and guidelines and deciding the degree of safety of Personal Data by considering the nature and dangers of Personal Data that should be ensured in the handling of Personal Data. The P2P Lending application is a data innovation that gives an immediate correspondence stage between one individual and another/P2P. Its application in every case straightforwardly gets to the Personal data of the individual who utilizes the application. Everything identified with data innovation can't ensure 100% information security. There will consistently be escape clauses. The execution of ISO/IEC 27001 is relied upon to limit this to keep up with the classification and security of the Application User's Personal Data. Numerous P2P applications offer direct admittance to your data and administrations... the P2P applications could have security openings, or ill-advised

organizations could make one... P2P raises genuine worries, yet nor movement or innovation is 100 safe.

As per the writer, P2P Lending Operators, a significant level Electronic System Operator dependent on Article 4 of the Communication and Information Technology No. 4 of 2016. There are 2 (two) reasons: first, on the grounds that P2P Lending Operators are needed to get ISO/IEC 27001 Certification, and second on the grounds that the P2P Lending application is an electronic framework that impacts the interests of explicit areas, as far as this is the monetary area.

#### 4 Conclusion

P2P Lending Operators are high-level Electronic System Operators because P2P Lending Operators must obtain ISO/IEC 27001 Certification. Second, the electronic system of P2P Lending Providers is an electronic system that impacts the interests of specific sectors, namely the financial sector. As a consequence of these two things, Personal Data obtained by the Operator must be kept safe, and information security management measures are carried out through the ISO/IEC 27001 standard. The implementation of this ISO/IEC 27001 standard ensures the achievement of Personal Data Security, namely the maintenance of confidentiality. ), Integrity, and Availability, and most importantly, security.

UU ITE, Perkominfo PDP, PP PSTE, and POJK No. 77, and the PDP Bill have all regulated the right of the Personal Data Owner to access. The Borrower, as the Owner of Personal Data, has the right to access his Data following the provisions of the legislation. Not only the right to get access, but the Borrower also has the right to get legal protection from unauthorized access and disclosure of his Personal Data. Any party that does not have a legitimate interest is not allowed to access the Personal Data of the Borrower.

#### References

- [1] E. E. Supriyanto, "Strategi Penerapan Kebijakan Sovereign Wealth Funds (SWFs) di Indonesia: Studi Literatur dan Studi Komparatif Oman," *J. Inov. Ilmu Sos. dan Polit.*, vol. 3, no. 1, p. 10, Apr. 2021, doi: 10.33474/jisop.v3i1.6959.
- [2] I. Wardhani and M. Barthos, "The Implementation of the Principle of Profit Sharing in the Musyarakah Financing Contract in Islamic Banks," 2021, doi: 10.4108/eai.6-3-2021.2306418.
- [3] Y. M. Manan, "The Role of Religiosity , Halal Awareness , Halal Certification , and Food Ingredients on Sistem Purchase Integrasi Proteksi & of Manajemen Resiko Intention Halal Food Platform Fintech peer to peer ( P2P ) Lending dan Payment Gateway untuk \* Meningkatkan," *Ihtifaz*, vol. 2, no. 1, 2019.
- [4] S. Chishti and J. Barberis, *The Fintech Book: The Financial Technology Handbook For Investor, Entrepreneurs And Visionaries*. John Wiley & Sons, 2016.
- [5] S. K. Shivakumar and S. Sethii, *Building Digital Experience Platforms: A guide to developin Next-generation Enterprise Applications*. APress, 2019.
- [6] M. H. Y. Purba, "Penguatan Perlindungan Konsumen dalam Industri Peer to Peer Lending di Indonesia," *Kanun J. Ilmu Huk.*, vol. 22, no. 3, pp. 547–566, 2020, doi: 10.24815/kanun.v22i3.17099.
- [7] N. Desideria, "Problematika Hukum Dalam Penggunaan Financial Teknologi,"

Universitas Pancasakti Tegal, 2021.

- [8] J. Sengupta, "Digital Banking in Asia Winning approaches in a new generation of financial services," *Asia Financ. Institutions*, pp. 1–89, 2014.
- [9] P. Sironi, *FinTech Innovation: From Robo-Advisors to Goal Based Investing and Gamification*. 2016.
- [10] S. A. Fitria, "Aspek Digital Lending di Indonesia," in *Jurnal Legislasi Indonesia*, vol. 17, no. 4, 2020, pp. 437–450.