Will Data Protection Act Change the Use of Data in Indonesia Financial Services?

Suwinto Johan

Faculty of Business, President University, Indonesia.
Jababeka Education Park, Jl. Ki Hajar Dewantara, RT.2/RW.4, Mekarmukti, North Cikarang, Bekasi Regency, West Java 17530 E-mail: suwintrojohan@gmail.com

Submitted: 14/12/2021 Reviewed: 23/02/2022 Accepted: 29/02/2022

Abstract: This data science examines a variety of data in order to aid humans in making complex decisions. This science aids management in making complex decisions. Artificial intelligence, machine learning, big data, and algorithms all fall under the category. Data science is growing in popularity as a result of the increasing reliance on technology by businesses such as social media companies and financial technology companies. Financial technology companies create applications that allow for the collection of consumer information. This information is transformed into a set of decision-making management tools. This information was easily obtained prior to the Personal Data Protection (PDP) Act’s enactment. This tool can assist management in becoming more efficient and effective in their operations. Additionally, this tool can be used to make complex management decisions, such as credit decisions for financial institutions and product marketing to consumers through appropriate advertising. The objective of this research is to examine use of data for business purposes after the enactment of the PDP Act. This study employs a descriptive and legal normative method. This research concludes that enacting the PDP Act will reduce the effectiveness of information processing. However, distinct information protection laws must be developed to improve consumer data protection. Additionally, public education about personal data protection needs to be strengthened. The PDP Act should regulate consumer protection issues and establish independent data protection institutions.

Keywords: Act; Data Science; Personal Data Protection

DOI: 10.32801/lamlaj.v7i1.297

INTRODUCTION

Hackers have stolen e-commerce customer and social media user data on multiple occasions. Personal data collection businesses must be able to safeguard their users’ personal information.¹ Up to 91 million users’ information from Tokopedia, an Indonesian e-com-

The WhatsApp application that collects personal data can use them to understand interests and lifestyles to support advertising strategies, form political stances, change the emotional state of customers, and determine the existence of advertisement accuracy and potential of personal data loss. This demonstrates the critical nature of personal data protection. Personal data protection is critical. This is in reference to Article 28 G, Paragraph 1 of the Republic of Indonesia’s 1945 Constitution. Personal dignity and property under its control, as well as the right to a sense of security and protection from threats to do or not do something, are all fundamental human rights. Personal data protection is a component of human rights.

Personal data has become increasingly crucial in line with the COVID-19 Pandemic. Many community activities are carried out digitally. Indonesia’s data protection, on the other hand, is in the spotlight due to the absence of a specific regulation. The digital economy has contributed US$ 100 billion to the distribution of goods and services and is ASEAN’s largest economy. The risk of personal data leakage is increasing in tandem with Indonesia’s rapid development of e-commerce. Tech companies have greater control over their users’ data than the government does. The government must enact regulations governing the collection, processing, and use of data.

Malaysia already has regulations governing the protection of personal data, which are enshrined in the 2010 Personal Data Protection Act. In Malaysia, the PDP Act does not fully protect the use of personal data. The protection of personal data is a fundamental right of European Union citizens. In today’s interconnected world, data protection regul-

---

tions (the General Data Protection Regulation, or GDPR) serve as the legal foundation for additional statutes.\textsuperscript{15} Personal data protection laws will render data science ineffective. Data science will face difficulties obtaining accurate data if consumer data is restricted, particularly in the financial industry.

The concept of a PDP regulatory approach is presented in the form of a code of conduct. It includes a statutory approach, a market-based solution, a technology approach, and a corporate privacy approach based on unique data rules.\textsuperscript{14} Machine Learning is used to perform automatic decision-making patterns at the moment. Humans make appeals to the outcomes of Machine Learning decisions. This pattern of decision-making must be reversed through human decision-making and machine appeals.\textsuperscript{15} Since the General Data Protection Regulation (GDPR) was implemented in 2016 and became effective in 2018, this act has generated numerous requests for a “right to explanation” for decisions made automatically or by an artificial intelligence algorithm. Since 2018, the European Union has mandated that the right to explanation be enforced.\textsuperscript{16} The Financial Services Authority (FSA), Bank Indonesia (Central Bank), and the Ministry of Communication and Information Technology regulate PDP in Indonesia. Indonesia does not have a law on the subject.\textsuperscript{17} On the other hand, the financial services authority has enacted regulations governing Know Your Customer (KYC) and the confidentiality of customer data.

In today’s digital economy, user data is a primary source of service advancement. Consumers who use this service provide service providers with personal information. Consumers rarely consider the ramifications of their data privacy. The data set also contains information about the users. At times, this results in unexpected consequences, such as unwanted advertisements and identity theft based on personal data.\textsuperscript{19} Personal data protection also has an impact on the implementa-

\begin{thebibliography}{99}
  


\end{thebibliography}
tion of online elections.\textsuperscript{20} Falsification of data has increased in popularity. Design science research is required to ensure the accuracy of personal data.\textsuperscript{21}

Establish firm and comprehensive legal rules that can protect personal data through electronic media in Indonesia.\textsuperscript{22} The analysis of big data and artificial intelligence (AI) has resulted in illogical and unverifiable conclusions and predictions about individuals’ behavior, preferences, and personal lives.\textsuperscript{23} The May 2018 General Data Protection Regulation (GDPR) is insufficient to safeguard personal data in the European Union.\textsuperscript{24}

Personal data protection requirements add to management’s and employees’ workloads. The execution of this regulation faces significant hurdles.\textsuperscript{25} In Indonesia, there are no clear policies governing personal data privacy for fintech P2P lending. Regulators must be able to guarantee that P2P lending will be able to comply with future regulations requirements.\textsuperscript{26}

Regulations governing the protection of personal data in Indonesia, as well as the Malaysian Law on the Protection of Personal Data, which governs the choices, purposes, and limitations in the use of people’s personal data so that user privacy rights are not violated.\textsuperscript{27} In order to develop particular legislation for the protection of personal data, Indonesia is benchmarking from Malaysia and making comparisons.\textsuperscript{28} Indonesia currently lacks comprehensive data protection legislation, whereas the United Kingdom and Malaysia have had such in place for a long period. As a result, criminals or threats of crimes such as cyber-attacks have emerged.\textsuperscript{29}


\textsuperscript{29} Vina Himmatus Sholikhah, Noering Ratu Fatheha Fauziah Sejati, and Diyanah Shabitah, “Personal Data Protection Authority: Comparative Study
The purpose of this research is to examine use of data for business purposes after the enactment of the PDP Act. Financial institutions have used consumer data to improve efficiency. Use of customer data to offer more appropriate products. Consumer information is processed to accelerate credit decision making through artificial intelligence.

This research focuses on PDP actions in light of current technological advancements, particularly in the field of data science, including machine learning, artificial intelligence, and other algorithms. Research that connects technological advancements, data science, and statutory regulation is still extremely rare. This research is unique in that it connects data science and law science. This research has a research question, namely whether enacting a PDP Act will result in the growth of data science, particularly in the financial services industry, and how to implement data science in the financial services industry while complying with consumer data protection laws. And how does the PDP Act regulate data usage in the absence of consumer consent? How do Malaysia’s personal data protection laws compare to those in place in Indonesia?

METHOD

The legal literature research or legal normative method is used in this research based on the background and previous studies. This study examines secondary sources, such as library materials. The literature review process entails the examination of legal principles and standards, as well as the examination and analysis of related legislative and regulatory systems. This research aligns existing laws and regulations governing the protection of personal data horizontally and vertically. The study of normative law employs a statute-based approach, in which all applicable laws and regulations pertaining to the protection of personal data and electronic transactions are analyzed. The research analyzes regulations pertaining to the use of personal data, identifies them, and adapts them. Primary legal materials, secondary legal materials, and tertiary legal materials or other supporting materials are all examples of normative legal research materials. The comparative law method is also used in this research. Comparisons of Malaysian and Indonesian legal systems are made.

ANALYSIS AND DISCUSSION

Enacting a Personal Data Protection Act Will Result at the End of Data Science

Individual consumer data is aggregated by service providers and financial technology companies. The data set contains a variety of consumer-related details. This type of data is referred to as big data. Following that, these data are grouped and tested for the presence of a variable. We will look for variables that affect a customer’s payment quality in financial technology companies. Data are grouped and analyzed using a variety of statistical models, including the binary logic test. Customer data on those who pay on time and customer data on those who become bad debts or non-performing loans. Machine learning is the process of analyzing this data. Statisti-

---

between Indonesia, United Kingdom, and Malaysia,” Indonesian Scholars Scientific Summit Taiwan Proceeding 3 (2021): 54–63.


cal or econometric models are validated using both existing variables and derivatives of the primary variables.

The more data entered, the more precise the prediction mode. Continuous data processing ensures that the predictive model remains precise over time. Adjustments to the model are required to account for changes in consumer behavior. This is referred to as the AI model. Risk management teams in financial technology companies can use this AI model to determine the type of prospective customer who is secure based on the data entered. Credit decisions become more efficient and timelier. Credit decision-makers’ subjectivity is dwindling. Figure 1 describes data processing as a basis for consumer decision making in financial institutions. Data is grouped and then evaluated to make business judgments.

Apart from making better decisions, financial technology companies’ work processes are becoming increasingly efficient. The number of workers employed is decreasing. A portion of the work was automated.

Additionally, models built with AI, machine learning, and big data have been used to forecast appropriate marketing or advertising based on consumer needs. A consumer uses the internet or a search engine to look up specific product information. The e-commerce application will then be able to identify and deliver advertisements to consumers, as well as provide information about specific products.

Additionally, models built with AI, machine learning, and big data have been used to forecast appropriate marketing or advertising based on consumer needs. A consumer uses the internet or a search engine to look up specific product information. Then the e-commerce application will be able to quickly determine and carry.

**Figure 1:** Stages of Processing Data Science

![Diagram showing stages of processing data science](image)

**Source:** research results
A person’s data can be classified into four categories: identity data that is permanently associated with a person, material data that is accessible to the public, material data that is accessible to the public but not accessible to the public, financial transaction data, and personal data stored on a mobile phone or device. Identity data, such as a person’s name, address, date of birth, national identification number, and taxpayer identification number, is immutable and cannot be changed except under specific circumstances. This information is also applicable to a business or corporation. Corporate data includes the corporation’s name, address, telephone number, board of directors, commissioner, and company document number.

The public has access to certain types of data, including a residential address, an office or a business address, telephone numbers, mobile phone numbers, email addresses, age, signature, work experience, educational status, and educational location. Although this data is material, it has an effect on the data owner. Data can be used for criminal purposes.

The public does not have access to the material data, which includes the maiden name of the biological mother, the title and number of emergency contacts, the name of a family physician, and health information. These data are known to close individuals rather than the data owner.

Financial data is a part of material data. Income data, debt balance data, asset data, bank account data, and debt account data are crucial. Financial data has always been material data for a person, especially income, debt, assets, and taxes imposed.

The application’s personal data reflects the user’s activities. These data include the most frequently visited locations, the commute route to work, the type of coffee most frequently ordered, the type of news most frequently read, and the political attitudes expressed through what is read. Table 1 describes the types of data that can be obtained from consumers. Consumer data that is simple to collect is presented in detail.

<table>
<thead>
<tr>
<th>No.</th>
<th>Data Type</th>
<th>Data Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a</td>
<td>Identity data and permanently attached to a person</td>
<td>Name, Place, and Date of Birth, Identity Number, Taxpayer Number, Social Security Identification Number (BPJS), Driver Identification Number</td>
</tr>
<tr>
<td>1b</td>
<td>Identity data and permanently attached to the company or corporation</td>
<td>Name, Address, Telephone Number, Name of Board of Directors, Name of Commissioner, Company Document Number</td>
</tr>
<tr>
<td>2</td>
<td>Public Material Data</td>
<td>Residential Address, Office Address, Phone Number, Email, Age, Signature, Work Experience, Education Status</td>
</tr>
<tr>
<td>3</td>
<td>Non-public Material Data</td>
<td>Mother’s Maiden Name, Name of Emergency Contact, Name of Doctor, Health Data</td>
</tr>
</tbody>
</table>
These data are then used to forecast an individual’s behavior. The data may be associated with a credit application submitted by an individual to a financial institution. Demographic, psychological, and financial information can all be used to forecast an individual’s debt behavior. Additionally, this data can reveal a person’s consumption habits. Additionally, these data can be used to perform a verification function.

The data on a person’s presence in a location from night to morning will reflect the person’s residence. The location of an individual in an area from morning to evening will reflect the location of his or her business. The news that is read can provide insight into a person’s political stance. The types of social media accounts followed by an individual can reflect their political views. A person’s financial capacity and ability are demonstrated by the number of transactions and financial value he or she makes.

The PDP Act’s enactment will restrict companies’ access to their customers’ data, particularly financial technology companies. If the PDP Act restricts the types of data that companies can use, data science will continue to be used. However, if the PDPA strictly restricts the types of data that can be used, it will be difficult for data providers and financial technology companies to use the data.

Even with this constraint, data science will be able to process customer data. This data is not always accurate due to the limited data types available: the more information available, the more accurate the prediction. With fewer data points, the prediction model will be less precise.

**Implement Data Science After Consumer Data Protection Laws**

Data science has altered the competitive landscape of business. Businesses that understand their customers will succeed in business. Businesses that use data mining, or what is referred to as big data, will be able to ascertain consumer behavior. Businesses will be able to predict consumer behavior using big data and an AI model. Apart from consumer behavior, businesses can also accelerate the process of customer service. The procedure could be enhanced. The more a company understands its customers, the more likely it is to provide adequate services to them. These businesses will see an increase in consumer purchases of goods and services.

Companies must comply with this regulation following the implementation of the PDP Act. Numerous businesses anticipated or complied with these PDP Acts. The company will obtain consent from consumers prior to using personal data. This consent should convey to the consumer an understanding of the purpose for data usage. The company must explain the purpose for which the data is being used. The consumer has the right to choose whether or
not their data may be used. Several large technology companies, including WhatsApp and Facebook, have taken this step. Consumers are prompted to confirm or approve the use of their data. If the consumer objects, the relationship is terminated. Uninstall the company’s application. If a business continues to do business with a customer, the business is not permitted to use consumer data. If consumers consent to the company’s use of their personal data, the company can better manage consumer expectations and provide superior company services. Figure 2 illustrates this.

**Figure 2: Consumers’ Consent Process**

![Diagram of Consumers’ Consent Process]

**Source:** research results

The aggregation of consumer data is referred to as big data. AI is created through the processing of large amounts of data. Additionally, machine learning is used to continuously improve big data. Machine learning will continue to analyze updated consumer data and make improvements. From artificial intelligence, we can continuously improve our service to consumers.

Thus, the PDP Act requires consumers to provide written consent to businesses for data usage. The business must create an authorization form for data usage. Consent to the use of this data must be incorporated into the sentence structure, font size, and agreement structure.

Consumer data approval requests must be appropriately regulated and verifiable to the parties concerned. Acceptance of this data should be documented and auditable. The following sections will discuss the various types of consent.

**Limits on the Use of Personal Data**

The PDP Act should specify the purpose for which data will be used. When data is obtained from a business, it must be used exclusively for business purposes. The data must be used solely for business purposes. In some countries, political campaigns are
the primary reason for the use of personal consumer data. The act must clearly define the act’s use of data. Additionally, the PDP Act must regulate the duration of data usage with consumer consent. Consent for the use of consumer data is not perpetual. Businesses will be required to obtain ongoing approval in order to develop more intelligent machine learning for AI. To safeguard consumers’ interests, the PDP Act requires the establishment of a consumer approval period. For the financial industry, the period during which consumer data is used is limited to the duration of the relationship. For instance, a consumer takes out a two-year loan. Then, consumer data may only be retained for a period of two years. Apart from the duration of data usage and the purpose for data usage, the PDP Act should impose restrictions on data usage permits. This data is only shared with companies with whom we have a direct relationship. The company may not disclose data to third parties. In some instances, businesses provide data to third-party data management firms. The data management company then utilizes it for additional purposes. Additionally, the PDP Act should regulate the use of aggregate data, rather than individual consumer data. Due to confidentiality concerns, consumer personal data may not be displayed. Aggregated data is not individual data; it is comprehensive data. Aggregated data does not reveal any personally identifiable information about consumers. Personal data about consumers may include their name, date of birth, identification number, mother’s maiden name, and other identifying information. Additionally, the government should establish an agency to oversee the use of this data. For the future, data is critical. The data control agency will be responsible for resolving disputes between consumers and businesses regarding the use of consumer data, supervising the use of consumer data by businesses, supervising the form of agreements between businesses and consumers, establishing time limits on the use of consumer data, and providing data usage certification or data security ratings. The PDP Act must establish standards for data users, particularly in critical industries. The financial sector, for example, is critical to the economy. This certification is based on the level of data security maintained by businesses or individuals. Each business must make public the data security rating assigned by the data monitoring organization. This will instill confidence in consumers when providing data to businesses. This rating will instill greater confidence and certainty in consumers and businesses. This rating should be a guarantee for consumers in providing data. Consumers will be calmer in doing business with this company. This rating can be in the form of a certification or rating or by noting that this institution or company is supervised and registered by the agency. The use of data is crucial, such as financial institutions being monitored by the Financial Services Authority or the broadcasting industry being monitored by broadcasting institutions. Data security certifications and ratings should be reviewed annually. Meanwhile, the purpose of monitoring surveillance will be to provide the ability to provide sanctions and revoke permits for data use. The government must enact data protection regulations, including the establishment of a data use monitoring agency. This organization will be required in the future. Data has evolved into a source of personal enrichment.
The individual with the most data will win the competition. In the early stages of the industrial revolution, data was transformed into a mineral source. Data mastery will trump business competition. In the business world, data mining has become a new source of revenue. Businesses that possess data mining capabilities will be able to outperform their competitors. Big data is the term used to describe this data mine.

Comparison of Personal Data Protection in Malaysia and Indonesia

Malaysia adheres to the principles of personal data protection as the OECD countries apply. These principles include the Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguard Principle, Openness Principle, Individual Participation Principle and Accountability Principle. Malaysia imposes a fine or a maximum prison term of five years or both. The law in Malaysia has been in effect since 2013. Malaysia has also established a Personal Data Protection Advisory Committee which is in charge of receiving complaints against personal data breaches. Meanwhile, the protection of personal data in Indonesia based on the Law on Information and Electronic Transactions has not regulated in detail and principles that must be obeyed by business actors. Indonesia has not specifically regulated the protection of personal data.

CONCLUSION

Commercial use of personal data has grown exponentially in technology companies, particularly in financial technology. Legal protection is required for the use of these personal data. Personal data can be exploited for economic gain. Each consumer must provide written consent for the use of their personal data. Consumers have a right to access their personal information. Authorities must rein in this trend by enacting legislation and regulations to safeguard personal data. Additionally, authorities must educate the public about the critical nature of personal data protection. The PDP Act should regulate consumer protection issues and establish an independent data protection institution. Research can be developed by conducting a survey of consumers and management of financial institutions. Research can be done by distributing questionnaires. Other research can be developed by examining the effectiveness of data use in financial institutions.

BIBLIOGRAPHY

Book Section

Journal
Ghani, Fadhilah Abdul, Syahirah Mohd Shabri, Maizatul Akmar Mohd Rasli, Nurulhuda Ahmad Razali, and Emir Hambali Ahmad Shuffri. “An Overview


Internet


CNBC. “Kacau Banget! Kok Bisa Sih Data Tokopedia Bocor?” CNBC Indonesia.


Proceedings


Johan, Suwinto. “Social Media Technology Firms or States : Who Knows the People Better ?” In Seri Seminar Riset II (Serina 2) Universitas Tarumanagara, 1–8, 2021.

Sholikhah, Vina Himmatus, Noering Ratu Fatheha Fauziah Sejati, and Diyanah Shabitah. “Personal Data Protection Authority: Comparative Study between Indonesia, United Kingdom, and Malaysia.” Indonesian Scholars Scientific Summit Taiwan Proceeding 3 (2021): 54–63.