International Journal of Global Community
Volume IV No. 1 (March), 2021

The Emergency over Private Data Protection Regulation for Users of Online Loan Services*

Shinta Hadiyantina, Dewi Cahyandari, Nandaru Ramadhan

Faculty of Law, Universitas Brawijaya, Malang, Indonesia,

Email: shinta_fh@ub.ac.id; dewicahyandari31@gmail.com;
ramadhannandaru@gmail.com

Abstract

One of the electronic transactions related to e-contracts that are currently developing involves information technology based lending and borrowing services, or commonly known as FinTech Lending, which offers various facilities for borrowing money. The convenience offered in lending and borrowing money based on information technology, on the other hand, raises problems, namely related to the protection of users' personal data. The problem is what is the appropriate legal protection model for personal data held by online loan providers in Indonesia. This study examines how the regulation of data protection in Indonesia is related to fintech activities. The model of legal protection for personal data mastered by online loan providers in Indonesia is to use legal protection from the law, namely the Personal Data Protection Act which is still at drafting stage. The law that is to be passed must contain the principles of good personal data protection, the establishment of an independent organization that is authorized to handle the protection of personal data, as well as detailing the matters that are owned by the subjects of data.

Keywords: personal data protection, fintech, Online Loan Services.

* This paper presented as Call for Paper on National Seminar on Urgency Protection of Personal Data in Digital Age. Held by Riksawan Institute in Hotel Redtop Jakarta, August 19, 2019.

Introduction

In today's technology digital era, many families dealing with a financial emergency find themselves searching for online loan options to get a cash. Usually, online loan is preferred by those who need quick cash or those who cannot borrow money from conventional loan services like banks, capital market, or other loan companies. This trend is made more obvious by the existence of the Internet that enables banking transaction. Internet has lured global economy into a whole new level, or commonly known as digital economic (Indrajit, 2001). In the era of digital economic development, people keep developing innovation to provide loan services like technology-based lending loan services that have contributed to national development and economy. Information technology has transformed people and given new business opportunities and new careers (Sjahdeini, 2001:1). This innovation has brought to the term electronic contract or commonly heard as e-contract.

In Indonesia, electronic contract is regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (hereinafter UU ITE), specifically in Article 1 point 17, which is further explained in Government Regulation Number 82 of 2012 concerning Administration of Electronic Transactions and System (hereinafter PP PSTE) in Article 1 point 15. Those two Articles contain the same definitions regarding e-contract, specifically regarding agreement for all parties concerned made based on electronic system.

Electronic system, based on Article 1 Number 5 UU ITE and Article 1 Number 1 PP PSTE, is a series of devices and electronic procedures functioning to prepare, collect, organise, analyse, save, display, announce, transmit, and/or disseminate electronic information. Prior to the Law Number 11 of 2008 concerning Electronic Information and Transactions and Government Regulation Number 82 of 2012 concerning Administration of Electronic Transactions and System, Indonesia had always referred to Civil Code/*Burgerlijk Wetboek* (BW) for its legal protection, as in Article 1313 suggesting that an agreement involves a person or more who are bound to another person or more (Satrio, 1992: 17).

According to Article 47 Paragraph (2) of Government Regulation Number 82 of 2012 concerning Administration of Electronic Transactions and System suggests that an electronic agreement is valid when:

1. there is agreement between parties;
2. it is made by competent or authorised legal subjects representing according to the provision of legislations;

3. there is a certain thing; and
4. the objects of the transactions must be relevant to existing legislations, morality, and public order.

One form of electronic transactions that is on the rise these days is information technology-based loan services or it is more popular with the term "Financial Technology" or FinTech Lending, giving services in money lending based on information technology. FinTech Lending emerged with the development of information technology, including the internet, smartphones, and big data analytics, which enabled faster and cheaper distribution of financial services. Fintech presents a challenge to incumbent financial institutions as it offers alternative services to post-global financial crisis society. However, it does not come without issues over protection of users' personal data.

Personal data protection is deemed fundamental, as it is regulated in Universal Declaration of Human Rights (UDHR) passed on 10th of December 1948 in Palais de Caillot, Paris in Article 12 that regulates every individual's rights to obtain protection, including that for every user's personal data. In Universal instruments, protection for personal data is implied in Article 17 of the Covenant concerning Civil and Political Rights (further stated civil and political rights covenant) that is agreed and openly signed. The validation and statement of General Assembly Resolution 2200 (XX1) were made on 16th of December 1966. Article 17 mentions legal protection linked with arbitrary and unlawful interference into personal confidentiality. The existence and basis of human rights seem to be for the sake of human being, meaning that every individual can earn from his/her human rights (Effendi, 1994: 47).

The concept of data protection is often treated as part of protection for the right to privacy. Regulatory model concerning protection for personal data can be elaborated as follows (Wahyudi, 2016: 8):

> "The regulation intended to serve as the mechanism of personal data protection within the structure of fulfilling the right to privacy can be seen from several regulatory models established by several parties, including international organisation such as European Region, OECD and APEC. Moreover, several personal data protection models also actively contribute to the regulatory models per se. Those regulatory models indicate how crucial personal data protection is for human rights. Regulatory models of personal data protection also involve an issue related with supervision over personal data processing. In addition, the mechanism to help victims whose personal data is violated to recover also becomes essential."

Data protection is principally linked with privacy as suggested by Alan Westin (1967: 7) who first defined private data or information privacy as a right held by individuals, groups, or agencies to decide on their own about when, how, and to what extent their personal information is disseminated or not to other parties. Principally, personal data has to be well protected, including that regarding general information, business information, government documents, intellectual property rights, health information, personal data in banking system, and personal identity (Supriyadi, 2017).

Personal data used in online loan services has not been appropriately protected. Companies have accessed people's data for companies' interests. Legal Aid Service Jakarta (LBH Jakarta) mentioned there were 1,330 grievances from victims of online loan services. The grievances were heard within 4 November to 25 November, LBH said. There were about 283 victims expressing their grievances over some violation.

Cited from official web of LBH Jakarta on Wednesday (7/11/2018), cases in online loan services have grown since June 2018, where collecting debt from customers is inappropriately performed. In reference to the grievances, the LBH Jakarta came to the first finding (Hartini, 2018):

a. Collecting debt involves mock, threat, denigration, and even sexual harassment;
b. Collecting debt involves calling all contacts related to the consumers/debtor such as the contact numbers of their bosses, parents-in-law, friends in primary school);
c. It charges considerably high interest rate and it is unlimited;
d. Personal data is unfairly accessed (contacts, text messages, calls, memory card, and so forth) from customers' cellular phones;
e. Collecting debt is done even before it is due and it is done anytime;
f. No call centres of online loan services is available for grievances;
g. No clear addresses of online loan services is available;
h. Application of online loan services changes name without any prior notification to customers while the interest rate keeps running despite the name change.

This issue will badly affect the victims of this services, where in some cases, some are traumatic and it even leads to suicide caused by depression due to inhuman debt collecting. On 11th of February 2019, a guy named Zul was found dead as he took his life and this case is connected to online loan services. Zul left a letter of apology addressed to his family. In the letter, Zul also requested that Financial Services Authority ban online loan services since he thought the services were 'an evil trap' and begged that no one would pay off the debt since he felt that it was his own responsibility (Waskita, 2019). Responding to this tragedy, Financial Services Authority suspected that the

suicide was connected to loan service from illegal fintech (CNN Indonesia, 2019). Moreover, Association of Fintech Indonesia and Association of Indonesian Fintech-based Joint Funding have suspected the same way where they believe that the loan service connected to suicide is illegal and not a member of association. In another case, a forty-year-old woman attempted suicide by drinking gasoline since she was trapped in IDR 500,000 debt from technology-based loan app (CNN Indonesia, 2019).

The two cases above are only a few of the negative impacts caused by online services. The big issue is related with access to users' personal data by the services, and it leads to contacting people close or once close to the debtor, in addition to another issue such as high interest rate. This research is more focused on the first research regarding accessing data in users' contact list on their phone to terrorise whoever the services can reach in case of bad credit. The problem raised is what is the appropriate model of legal protection for personal data controlled by online loan services in Indonesia?

Discussion

Personal Data

Digital era has triggered the explosion of personal data, saved and transmitted through computer and mobile devices, broadband, and Internet sites and media (Shiling, 2011: 1). This advanced technology could lead further to a serious issue impacting personal data and information security of the data. Information on individuals is always processed by government and private sectors, but computer era has even dragged it deeper into a more serious threat where the privacy of every individual is trespassed. Even worse, the debtors will face mounting consequences due to carelessness and the leak of information caused (Marrett, 2002: 95).

Data is defined as "a piece of information processed by means of an automated device that responds to instructions used accordingly and saved for processing." Data can be in the form of information on medical, educational, and social work-related reports, or any information saved as part of relevant data saving (Purwanto, 2007: 13). Furthermore, based on Article 1 point 27 of Government Regulation of Number 82 of 2012 concerning Electronic Administration of Electronic Transactions and system (PTSE), personal data is described as "particular individual data that is saved, and its truth and confidentiality are well kept."

Electronic Fund Transfer (EFT) is aimed to protect the security of national data that blocks access to national data saved in computer owned by the US Government (Gerald, 2004: 271). The term data protection was first used in Germany and Sweden back in the 1970s where personal data was

regulated in the law (Dewi, 2009: 37). Every country uses different term for personal information and personal data. Several countries like those in European Union and Indonesia use another term. Indonesia, for example, based on Law concerning Electronic Information and Transactions (UU ITE), uses personal data, but none specifies the type of the personal data. The US, Canada, and Australia use the term personal information (Dewi, 2009: 71). Protection for personal data including the legal protection, is guaranteed by the Law. In Indonesia, protection for personal data is stipulated in the Law.

Appropriate Model of Legal Protection for Personal Data Controlled by Online Loan Service Providers in Indonesia

Data is a piece of information processed via a device functioning automatically to respond to instructions used accordingly and saved for processing (Marrett, 2002: 95). Data is defined as information and as part of medical, social-related, education records or information that is saved as part of a relevant saving system (Purwanto, 2007: 13). Personal data is defined as connected information used to identify or can identify a person. This is not only restricted to written information, but it also involves photographs, visual images /audio, and recorded voice of a person or recorded voice that can identify a person (Makarim, 2005: 66).

Data protection was first used in Germany and Sweden back in the 1970s as a term that regulated personal data protection in the Law (Makarim, 2005: 66). In 1980, Committee of Ministers of Organization for Economic Cooperation and Development / OECD) released Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The guidelines contain basic principles concerning data protection and free flow of information among the states with laws relevant to the principles of data protection (Makarim, 2005: 151). In the following year, Council of Europe announced a convention concerning protection for individuals in automated personal data processing in "*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*". This convention was effectuated in 1985 and has the content similar to the guidelines mentioned earlier, but it is more focused on complexity of data protection to protect a person's privacy.

On the 20th of February 1995, the Committee of Ministers approved the design previously changed to an instruction (directive) further mentioned as "*Directive 95/46/EC of The Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*." This Directive was validated on the 24th of October 1995 and was effectuated in the next three years in 1998 following the validation. The Directive requires fifteen countries in European Union to stipulate the regulations regarding personal data processing (*processing of*

personal data). The parties regulated in the Directive consist of (Makarim, 2005: 67):

a. The subject of data, or a person whose data will be processed;
b. Controller, or a person or an organisation that is authorised to independently or jointly set a goal or determine a way to process the data as required by the state or the law. Controller is determined by the state or the law;
c. Processor, or a person or a legal entity, state organisation, or agency or another form of organisation processing personal data on behalf of the controller.
d. Third party, or a person or a legal entity other than public authorities, an agency outside the subject of the data, controller, processor, or another person under the authority of controller or processor authorised to process data;
e. Recipient, or a person or a legal entity, public authorities, agency, or another organisation that access to data can be opened for.

Supervisory authorities, independent public organisations have authority to supervise the protection of personal data and to conduct enquiry into data processing activities, including the right to access data and authority to ban data transmitting to third parties. Grievances expressed by subject of data are received by this agency, and this agency has to make a yearly report according to the Law regulating protection (Makarim, 2005: 67).

In personal data protection, there are several principles intended to restrict data collection, data quality, specification of intention of use of restriction, security measures, publication of individuals' participation, and responsibilities. The principles involve the following (Dewi, 2015: 30):

a. Restriction of data collection: there should be restriction in personal data collection. Data is obtained according to appropriate legal procedures, and data collection requires knowledge and approval from an individual concerned during data collection.
b. Data quality: personal data must be accurate according to the objective of the data used, or it has to be complete and accurate.
c. Specification of objective: the objective of data collection must be specifically defined, involving what the data is for, and the use of the data must be relevant to the objective mentioned.
d. Use of restriction: data opened or made available for public or used for external purposes must be based on approval of the data owners.
e. Security measures: each data collected must be protected and protected from any risk of damage, change, open access without consent, or loss.

f. Openness: the data opened for general purposes or other purposes must be based on public policy.
g. Individuals' participation: each individual submitting his/her personal data for data collection has his/her right to obtain information on his/her own data or to delete or fix incorrect information of the data.
h. Responsibilities: any parties responsible for the data submitted must comply with the principles mentioned.

In Article 6 of Directive 95/46/EC of The Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, the principles of data protection are regulated as follows (Dewi, 2015: 170):

1) personal data must be processed in honest and lawful way;
2) personal data must be collected for specific purposes, explicitly and lawfully, and it must not be processed further in a way not relevant to the objective. Further data processing is conducted for the sake of history, statistics, and for scientific ground along with the protection given;
3) data collection must be relevant (sufficient), and it must not be exaggerated and must be in line with the objective of data collection and further processing;
4) data must be accurate and up-to-date; inaccurate, irrelevant, and incomplete data may be deleted or limited.
5) Data must be saved based on the intention of data collection and processing, and it must not be saved exceeding the time set.

One of the principles of personal data management in European countries is by managing the flow of personal data and banning personal data transmission outside the European Countries under the condition where the third country does not have any law relevant (*adequacy*) to those in European Countries, which could hamper international trade and businesses that have gone global (Dewi, 2017: 117). To anticipate the condition, OECD issued Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Llyodm, 2014: 31), within which there are six basic principles regarding data protection:

1) Collection limitation principle
   There must be limitation in personal data collection obtained fairly and lawfully, and it must be followed by agreement from the subject of data and must be with the consent of the data owner.
2) Data quality

The data obtained must match the objective of the use, and the personal data must be complete, accurate, and data must be immediately updated when there is any change of data information.

3) Purpose specification principle
   The purpose of personal data collection must be informed to the owner in the time when personal data is submitted. Furthermore, it is restricted to the objective.
4) Approval of the personal data owners is needed to disclose, provide, or use the data for another purpose of the data collection.
5) Security Safeguard principle
   Personal data deserves protection from any possible risk of data loss, data damage, use without consent, data disclosure, or any unlawful access.
6) Openness principle
   The main objective of data use, identity, and data control must be made. Prior to the objective making, a policy concerning openness in the development and processing of personal data must be made.

From the above principles, the urgency in the Law concerning personal data protection is getting clearer. In Indonesia, there is a policy massively collecting personal data of the population, like what has been done by e-commerce companies. People have to be informed about the data use and data processing regarding the data they submit.

Several countries have provisions specifically regulating the protection of the population personal data. Regarding to study by People Advocacy and Study Organisation (ELSAM) from 88 countries listed, fifty-seven of them have the Law specifically regulating personal data protection and thirty-one of them do not have any law regulating personal data (ELSAM, 2017). Moreover, ELSAM divides the power of personal data protection in each country into four categories:

1. Limited (L) represents the status of protection of the regulation whose implementation is at its weakest level. Personal data protection is only mentioned in one or two Articles in the constitution or state's regulation generally or it is not mentioned at all.

2. Moderate (M) represents the state protection of the regulation whose implementation is at its moderate level. The personal data protection of this status is not specific under one legal protection while the personal data protection is distributed to several private sectors or regulations of law enforcement.

3. Robust (R) represents status of state protection of regulation whose implementation is at robust level. This status has specific data protection as a law concerning personal data protection and its following regulations that do not refer to EU Data Protection Directive 95/46/EC.

4. Heavy (H) represents the status of state protection of the regulation whose implementation is at strong and heavy level since it has given legal consequence concerning personal data misuse. Protection of personal data refers to EU Data Protection Directive 95/46/EC, which was further implemented or ratified in a separate national regulation and is applicable.

The status is listed as follows (ELSAM, 2017):

Table 1
Status of Personal Data Protection in Various Countries

No.	Country	Regulation of PDP	Status	No.	Country	Regulation of PDP	Status
1.	Angola	Applied	M	45.	Macao	Applied	M
2.	Argentina	Applied	R	46.	Macedonia	Applied	M
3.	Australia	Applied	R	47.	Madagascar	Applied	L
4.	Austria	Applied	H	48.	Malaysia	Applied	M
5.	Bahrain	Applied	M	49	Malta	Applied	M
6.	Belarus	Applied	M	50.	Mauritius	Applied	M
7.	Belgium	Applied	H	51.	Mexico	Applied	M
8.	Brazil	Applied	L	52.	Monaco	Applied	R
9.	British Virgin Island	None	L	53.	Montenegro	Applied	M
10.	Bulgaria	Applied	M	54.	Morocco	Applied	R
11.	Canada	Applied	H	55.	Netherlands	Applied	H
12.	Cape Verde	Applied	M	56.	New Zealand	Applied	R
13.	Cayman Island	None	M	57.	Nigeria	None	M
14.	Chile	Applied	M	58.	Norway	Applied	H
15.	China	Applied	M	59.	Pakistan	None	M
16.	Colombia	Applied	M	60.	Panama	Applied	L
17.	Costa Rica	Applied	M	61.	Peru	Applied	M
18.	Croatia	Applied	M	62.	Philippines	Applied	L
19.	Cyprus	Applied	R	63.	Poland	Applied	H

20.	Czech Republic	Applied	R	64.	Portugal	Applied	H
21.	Denmark	Applied	R	65.	Qatar	Applied	M
22.	Egypt	None		66.	Rumania	Applied	R
23.	Estonia	Applied		67.	Russia	Applied	M
24.	Finland	Applied	R	68.	Saudi Arabia	Applied	M
25.	Germany	Applied	H	69.	Serbia	Applied	R
26.	Ghana	Applied	M	70.	Seychelles	Applied	L
27.	Gibraltar	Applied	M	71.	Singapore	Applied	R
28.	Greece	Applied	R	72.	Republic of Slovakia	Applied	R
29.	Guernsey	None	M	73.	South Africa	Applied	M
30.	Honduras	Applied	L	74.	South Korea	Applied	H
31.	Hong Kong	Applied	H	75.	Spain	Applied	H
32.	Hungary	Applied	R	76.	Sweden	Applied	H
33.	Iceland	Applied	R	77.	Swiss	Applied	R
34.	India	Applied	L	78.	Taiwan	Applied	R
35.	Indonesia	None	L	79	Thailand	None	L
36.	Ireland	Applied	H	80.	Trinidad Tobago	Applied	L
37.	Israel	Applied	R	81.	Turkey	Applied	L
38.	Italy	Applied	H	82.	United Arab Emirates	Applied	M
39.	Japan	Applied	R	83.	Ukraine	Applied	M
40.	Jersey	Applied	M	84.	Great Britain	Applied	H
41.	Latvia	Applied	R	85.	United States	Applied	H
42.	Lesotho	None	L	86.	Uruguay	Applied	M
43.	Lithuania	Applied	M	87.	Venezuela	None	L
44.	Luxemburg	Applied	R				

In Indonesia, the regulation concerning personal data is not specifically stipulated in the law, but some Articles are found in some laws regulating personal data:

Table 2
Laws regulating Personal Data Protection

Law	Article	Content
Law No. 36 of 1999	40	"Every person is prohibited, in any form,

concerning Telecommunication		from eavesdropping any information channelled through telecommunication network"
	42 Par. (1)	The telecommunication service operator is obligated to keep confidential the information transmitted and/or received by a telecommunication service subscriber through the telecommunication network and/or telecommunication services provided.
	42 Par. (2)	For the purposes of criminal prosecution, the telecommunication service operator is allowed to record the information transmitted and/or received by the telecommunication service operator and to provide information required on the basis of: a. a written request from the Attorney General and/ or the Chief of Indonesian Police for certain criminal offenses; b. the request of an investigator for certain criminal offenses in accordance with prevailing laws.
	42 Par. (3)	Provisions concerning the procedures for requests and submission of the recorded information referred to in paragraph (2) shall be regulated by Government Regulation.
Law No. 8 of 1981 concerning Criminal Law	47 Par. (1)	An investigator shall have the right to open, examine and seize other documents sent through the post and telecommunication office, communication or transportation agency or enterprise, if the goods in question are, for good reason, suspected of having a connection with a criminal case currently being examined, with a special warrant issued for such purpose by the head of the district court.
	47 par.	For such purpose, the investigator may

	(2)	request the head of the post and telecommunication office, the head of the communication or other transportation agency or enterprise concerned to surrender the intended documents to him, for which a receipt must be provided.
Law No. 36 of 2009 concerning Health	57 par. (1)	Every person has his/her rights to his/her health condition confidentiality as informed by health care providers.
	57 par. (2)	Provisions concerning rights to health condition confidentiality as referred to in paragraph (1) is required on the basis of: a) statutory order; b) court order; c) consent of the person concerned; d) interests of society; e) interests of the person concerned.
Law No. 11 of 2008 concerning Electronic Information and Transactions	26 par. (1)	Unless provided otherwise by rules, use of any information through electronic media that involve personal data of a person must be made with the consent of the person concerned.
	26 par. (2)	Any person whose rights are infringed as referred to in paragraph (1) may file a claim for damages incurred under this Law.

In terms of data protection, Indonesia has effectuated Article 42 of Law concerning Telecommunication whose Articles mention personal data protection, such as Article 40 regulating prohibition of eavesdropping, Article 42 Paragraph (1) concerning requirement for telecommunication providers to keep information sent by users confidential, and Article 42 Paragraph (2) and (3) concerning personal data in criminal transition process. Moreover, in Law concerning Telematics, Law Number 8 of 1981 concerning Criminal Procedures also contains several Articles mentioning personal data protection. This is obvious in Article 47 Paragraph (1) and Paragraph (2), regulating rights of the investigator to access recorded information approved by the head of court.

In Law Number 26 of 2009 concerning Health, Article 57 Paragraph (1) and (2) implies that every person has his/her rights to keep his/her health condition confidential. Similar regulation can also be found in Law concerning Electronic Information and Transactions mentioning personal data protection, specifically regulated in Article 26 Paragraph (1), stating that each piece of information through electronic media containing personal data of a person must be used with the consent of the person concerned, and in Paragraph (2) stating that when the rights as referred to in Paragraph (1) are infringed, one can file a claim for damages incurred under this law.

In fact, in addition to the Articles mentioned above, there are approximately 30 laws regulating personal data protection. However, the regulations given in those laws are still general and they do not completely provide protection for personal data. Another issue is related to the absence of law concerning personal data protection, where laws providing any recovery for those whose privacy is trespassed are minimum.

In addition to several laws with Articles concerning personal data protection, the regulation of Minister of Communication and Informatics Number 20 of 2016 concerning Personal Data Protection in Electronic System was also passed. However, the legal force given in the minister regulation is not as strong as that in the laws. Recalling that the minister's authority is executorial, the regulations made by ministers only give sanctions, majorly administrative ones, but they do not detail the mechanism of protection given for personal data. Thus, they are not able to appropriately protect personal data controlled by e-commerce companies.

The best protection model is by passing Law concerning Personal Data Protection. The need for law is intended to complete personal data protection where the regulations have been mentioned in several Articles in other regulations. The protection is intended to protect individuals' rights in the society regarding increasing incidence of tort related with personal data ranging from collecting, processing, to personal data distribution. Moreover, it is needed for the interests of the people without having to feel worried about any misuse that would violate their rights (Wahyudi, 2016). To date, the law on personal data protection is at drafting stage in the form of bill.

The principle that can be implemented in the bill concerning personal data protection is the principle made by OECD as the basis for personal data protection. The OECD has issued Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (Llyodm, 2014, p. 31). There are six basic principles of data protection in OECD:

a. Collection limitation principle is regarding the limitation in collecting personal data and the data must be lawfully and justly obtained and it must be with consent and approval of the subject of the data.
b. Data quality

Personal data must be relevant to the objective of its use and, for purposes as needed, data must be accurate, complete, and updated.

c. Purpose specification principle
   The objective of personal data collection must be decided in time of data submission and further use of the data is restricted to the fulfilment of the objective.
d. Personal data cannot be disclosed, provided, or used for purposes without any consent of the subject of data and without any law.
e. Security safeguard principle
   Personal data must be protected through acceptable protection and security against risks such as data loss or invalid access, damage, use, modification, or data disclosure.
f. Openness principle
   There must be public policy concerning openness towards development, practice, and policy regarding personal data, meaning that the existence and main objective of use, identity, and controlling centre of the data must be developed.

Another element that has to be applied in the bill concerning personal data is an Article regulating the establishment of an independent organisation specifically dealing with personal data protection and having integrity like in Malaysia and Singapore. The organisation is like a particular commission dealing with corruption in Indonesia whose authorities and existence are required by law. Moreover, the overlapping meaning of the concept of personal data must be fixed, since the concept serves as the key to breaking down the overlapping regulations caused by unclear concept of personal data protection in each law.

Explanation on details regarding the rights owned by the subject of data must also be given. Regulations concerning sanction imposition need to be improved and made clearer since they deal with private and civil rights of each citizen. Therefore, privacy and issues over personal data protection have been listed in agenda since they have urgency. It is also because many countries have implemented specific regulations concerning personal data protection.

Conclusion

The appropriate model of legal protection for personal data controlled by online service providers in Indonesia is based on legal protection derived from the law, specifically Law concerning Personal Data Protection that is still at its drafting stage or as bill. The law that will be passed must contain good principles of personal data protection, establishment of an independent

organisation authorised to deal with personal data protection, and details of the subject of the data.***

References

CNN Indonesia. 2018. *Tangis Korban Percobaan Bunuh Diri Terjerat Utang Fintech* (Cries of Suicide Attempted Victims entangled in Fintech Debt) Retrieved from https://www.cnnindonesia.com/nasional/20181105025234-12-343957/tangis-korban-percobaan-bunuh-diri-terjerat-utang-fintech (Demand 18.07.2019).

CNN Indonesia. 2019. *OJK Duga Korban Bunuh Diri Pinjam Uang dari Fintech Ilegal* (OJK Alleged Suicide Victims Borrowed Money from Illegal Fintech). Retrieved from https://www.cnnindonesia.com/ekonomi/20190213200418-78-369043/ojk-duga-korban-bunuh-diri-pinjam-uang-dari-fintech-ilegal (Demand 15.07.2019).

Dewi, Sinta. 2009. CyberLaw: *Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional* (Protection of the privacy of personal information in e-commerce according to international law) Bandung: Widya Padjajaran.

Dewi, Sinta. 2015. CyberLaw: *Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional* (Aspects of Private Data According to International, Regional and National Law). Bandung: PT Refika Aditama.

Dewi, Sinta. 2017. Model Regulation for Data Privacy in the Application of Biometric Smart Card. Brawijaya Law Journal Vol 4.

Effendi, Mahsyur. 1994. *Dimensi/Dinamika Hak Asasi Manusia Dalam Hukum Nasional dan Internasional* (Dimensions / Dynamics of Human Rights in National and International Law). Jakarta: Ghalia Indonesia.

ELSAM, 2017. Perbandingan Kewajiban Registrasi SIM Card dengan Perlindungan Data Pribadi di Berbagai Negara (Comparison of SIM Card Registration Obligations with Personal Data Protection in Various Countries) Source: https://referensi.elsam.or.id/wp-content/uploads/2017/10/ Perbandingan-Kewajiban-Registrasi-SIM-Card-dengan-Perlindungan-Data-Pribadi-di-Berbagai-Negara.pdf.

Gerald, Ferrera R. 2004. CyberLaw Text and Cases. South Western: Trejo Production.

Government Regulation of Republic of Indonesia Number 82 of 2012 concerning Administration of System and Electronic Transactions.

Hartini, V. 2018. *Dampak Buruk Pinjaman Online, Bikin Konsumen Trauma hingga Ingin Bunuh Diri* (Bad Impact of Online Loans, Trauma to Consumers Want to Suicide) Retrieved from https://www.liputan6.com/tekno/read/3686308/dampak-buruk-pinjaman-online-bikin-konsumen-trauma-hingga-ingin-bunuh-diri (Demand 13.07.2019).

Indrajit, R. E. 2001. E-Commerce: *Kiat dan Strategi Bisnis di Dunia Maya* (Cyber Business Tips and Strategies). Jakarta: Gramedia.

Llyodm, Ian. J. 2014. Information Technology Law. United Kingdom: Oxford University Press.

Makarim, Edmon. 2005. *Pengantar Hukum Telematika* (Introduction to Telematics Law). Jakarta: Rajawali Press.

Marrett, Paul. 2002. Information Law In Practice: 2nd Edition. Cornwall: MPG Books Ltd.

Purwanto. 2007. *Penelitian tentang Perlindungan Hukum Data Digital* (Research on the Legal Protection of Digital Data). Jakarta: Badan Pembinaan Hukum Nasional.

Satrio, J. 1992. *Hukum Perjanjian* (The Law of Contract). Bandung: Citra Aditya Bakti.

Shiling, C. G. 2011. Privacy and Data Security: New Challenges of the Digital Age. New Hampshire Bar Journal.

Sjahdeini, S. R. 2001. *Hukum Siber Sistem Pengamanan E-commerce* (Cyber Law E-commerce Security System). Presented at Seminar on the Role of Legal Enforcer concerning Banking Transaction, organized by Mandiri Bank on Thuesday, 18 Januari 2001 in Mandiri Club Jakarta.

Supriyadi, Daniar. 2017. Personal and Non-Personal Data in Context of Big Data. Unpublished Thesis. Tilburg University.

Wahyudi, et.al. 2016. *Perlindungan Data Pribadi: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia* (Protection of Personal Data: Proposed Institutionalization of Policy from a Human Rights Perspective). Jakarta: Elsam.

Waskita, F. 2019. *Sopir Taksi Gantung Diri Gara-gara Utang: Jebakan Setan Pinjaman Online dan Pesan untuk Rentenir* (Taxi Drivers Hang Yourself Over Debt: Devil's Trap Online Loans and Messages for Moneylenders). Retrieved from https://jakarta.tribunnews.com /2019/02/12/sopir-taksi-gantung-diri-gara-gara-utang-jebakan-setan-pinjaman-online-dan-pesan-untuk-rentenir (Demand 15.07.2019).

Westin, A. F. (1967). *Privacy and Freedom.* London: Atheneum.