Type: CIRCULAR LETTER (SE)

By: DEPUTY CHAIRPERSON OF THE BOARD OF COMMISSIONERS OF FINANCIAL SERVICE AUTHORITY

Number: 18/SEOJK.02/2017

Date: 18 APRIL 2017 (JAKARTA)

To: THE HONORABLE.
1. ADMINISTRATOR OF INFORMATION TECHNOLOGY-BASED MONEY LENDING SERVICES; AND
2. USER OF INFORMATION TECHNOLOGY-BASED MONEY LENDING SERVICES,

ON SITE.

Title: GOVERNANCE AND MANAGEMENT OF INFORMATION TECHNOLOGY RISKS IN INFORMATION TECHNOLOGY-BASED MONEY LENDING SERVICES

With reference to the entry into force of Regulation of Financial Service Authority Number 77/POJK.01/2016 regarding Information Technology-Based Money Lending Services, it is necessary to regulate implementing provisions regarding Governance and Management of Information Technology Risks in Information Technology-Based Money Lending Services in the following Circular Letter of Financial Service Authority:

I. GENERAL PROVISION

1. Financial Service Authority, hereinafter abbreviated as OJK, shall be independent institution, having the function, duties, and authorities of regulation, supervision, audit, and investigation as referred to in Law Number 21 Year 2011 regarding Financial Service Authority.

2. Information Technology-Based Money Lending Services shall be organization of financial services to bring together the lender and loan recipient in the framework of executing lending agreement in rupiah currency directly through the Electronic System by using the internet network.

3. Electronic System shall be series of electronic devices and procedures functioning to prepare, collect, manage, analyze, store, display, announce, deliver, and/or disseminate Electronic Information in the field of financial services.

4. Administrator of Electronic System shall be every person, state administrator, business entity, and public that provides, manages, and/or operates the Electronic System individually as well as jointly to user of Electronic System for its own interests and/or interests of other party.

5. Information Technology shall be a technique to collect, prepare, store, process, announce, analyze, and/or disseminate information in the field of financial services.

6. Administrator of Information Technology-Based Money Lending Services, hereinafter referred to as Administrator, shall be Indonesian legal entity that

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.

provides, manages, and operates the Information Technology-Based Money Lending Services.

7. User of Information Technology-Based Money Lending Services, hereinafter referred to as User, shall be lender and loan recipient using the Information Technology-Based Money Lending Services.

8. Board of Directors:

   a. for Administrator in the form of legal entity of Limited Liability Company shall be Board of Directors as referred to in Law Number 40 Year 2007 regarding Limited Liability Company; or

   b. for Administrator in the form of legal entity of cooperative shall be management as referred to in Law Number 25 Year 1992 Regarding Cooperatives.

9. Commissioner:

   a. for Administrator in the form of legal entity of Limited Liability Company shall be commissioner as referred to in Law Number 40 Year 2007 regarding Limited Liability Company; or

   b. for Administrator of in the form of legal entity of cooperative shall be supervisor as referred to in Law Number 25 Year 1992 regarding Cooperatives.

10. Electronic Transaction shall be legal action that is performed by using computer, computer network, and/or other electronic media as referred to in Law Number 11 Year 2008 regarding Electronic Information and Transaction.

11. Electronic Certificate shall be electronic certificate that includes Electronic Signature and identity showing the status of legal subject of the parties in Electronic Transaction issued by the Administrator of Electronic Certification as referred to in Law Number 11 Year 2008 regarding Electronic Information and Transaction.

12. Electronic Signature shall be signature that consists of Electronic Information adhered, associated, or related to other Electronic Information used as verification and authentication tool as referred to in Law Number 11 Year 2008 regarding Electronic Information and Transaction.

13. Administrator of Electronic Signature shall be legal entity functioning as the trusted party that facilitates the production of Electronic Signature.

14. Data Center shall be a facility used to place the Electronic System and relevant components for the purpose of placement of data storage and processing.

15. Disaster Recovery Center shall be a facility used to recover the data or information as well as important functions of Electronic System that are disrupted or damaged by the occurrence of disaster caused by nature or human.

16. Disaster Recovery Plan shall be document containing plans and measures to replace and/or recover the data access, required hardware and software, for the

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.

Administrator can run the critical business operational activities after the occurrence of interference and/or disaster.

II. ROLES AND RESPONSIBILITIES OF THE BOARD OF DIRECTORS

1. Board of Directors shall perform supervision to the Information Technology risks and shall ensure the function of Information Technology is capable to support the business strategies and objectives of the Administrator.

2. Board of Directors shall be responsible to the Information Technology risks arising from the activities, at least, including:

   a. making decision related to Information Technology;
   b. transfer management of Information Technology;
   c. security of Information Technology;
   d. protection of data and information; and/or
   e. management of Information Technology services.

3. Board of Directors shall prepare the framework of Information Technology risk management.

4. Board of Directors shall be responsible to the performance of Information Technology risk management in order to be safe, trusted, sustainable, and stable.

5. Board of Directors shall be responsible to the quality of product and service information submitted to User by taking into account the principles of, at least, including:

   a. openness;
   b. accuracy;
   c. objective;
   d. reliability;
   e. availability;
   f. comprehensible;
   g. integrity; and
   h. completeness.

III. DATA CENTER AND DISASTER RECOVERY CENTER

A. Placement of Data Center and Disaster Recovery Center

Administrator shall place the Electronic System in Data Center and Disaster Recovery Center in the territory of Indonesia in accordance with the applicable laws and regulations.

B. Disaster Recovery Plan

1. Administrator must prepare Disaster Recovery Plan for the operational continuity of Administrator can still be operating during the occurrence of disaster and/or disruption in the Information Technology facilities used by the Administrator.

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.

2. Administrator may perform trial upon the Disaster Recovery Center to the overall application and critical infrastructures in accordance with the Disaster Recovery Plan.

3. Administrator shall perform review of Disaster Recovery Plan at least 1 (one) time in 1 (one) year.

4. Administrator shall submit annual report related to Disaster Recovery Plan and Disaster Recovery Center to the Chief Executive Supervisor of Insurance, Pension Fund, Financing Institution, and Other Financial Service Institution.

IV. GOVERNANCE OF ELECTRONIC SYSTEM AND INFORMATION TECHNOLOGY

A. Electronic System Strategic Plan

1. Administrator shall register itself as Administrator of Electronic System at the Ministry of Communication and Informatics of the Republic of Indonesia.

2. Administrator must prepare and has Electronic System strategic plan that supports the business plan of Administrator.

3. Electronic System strategic plan as referred to in figure 1 must be included in the business plan of Administrator.

4. Electronic System strategic plan of Administrator shall be, among others, related to policies, procedures, and standards including at least aspects of:

   a. management;

   b. development and planning;

   c. operational of Information Technology;

   d. communication network;

   e. information security;

   f. Disaster Recovery Plan;

   g. User service; and

   h. use of Information Technology service provider.

5. Policies, procedures, and standards that have been prepared must be socialized to the employees as well as interested parties.

6. Policies, procedures, and standards that have been prepared must undergo periodic review to ensure the effectiveness and sufficiency.

B. Human Resources

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.

1. Administrator shall be obligated to have human resources possessing skills and/or background in the field of Information Technology.

2. Administrator must prepare human resources planning and the need for competence in the field of Information Technology.

3. Administrator must ensure that the competition required can be fulfilled well to guarantee the operational continuity of Administrator.

4. Administrator must improve the human resources quality and capacity of Administrator whether through education and training activities related to the organization of Information Technology as well as business process and service offered.

C. Information Technology Change Management

1. Administrator must have procedures that manage every change occurred in the electronic business process and system.

2. Administrator must determine the division of responsibility in managing every change occurred in the electronic business process and system.

3. Administrator must ensure every change occurred in the electronic business process and system has acquired formal approval.

4. Administrator must be able to control every change occurred in the electronic business process and system.

5. Administrator must document as well as deliver to the Chief Executive Supervisor of Insurance, Pension Fund, Financing Institution, and Other Financial Service Institution periodically every 3 (three) months at the latest on date 30 or in the occurrence of change in the electronic business process and system.

6. In the event that date 30 as referred to in figure 5 falls on holiday, therefore, delivery shall be made at the latest of 1 (one) next business day.

7. Administrator must perform separation between the operational zone and development in order to ensure that each change occurred does not disrupt the operational of Electronic System.

8. Administrator must ensure the personnel accessing documented operational zone and has acquired approval of the Board of Directors.

V. TECHNOLOGY MANAGEMENT TRANSFER

1. Administrator may use provider of Information Technology management transfer to support business activities of Administrator.

2. Provider of Information Technology management transfer shall be among others provider engaged in the field of system development service, maintenance

service, operational support service, network administration service, disaster recovery service, and cloud computing.

3. In the event that the Administrator uses the provider of Information Technology management transfer, Administrator shall have full responsibility to the risks occurred from and in the transferred management of Information Technology.

4. The use of provider of Information Technology management transfer must take into account the principles of prudential, continuity, and risk management that include at least:

   a. risks related to the use and/or acquisition from Electronic System by taking into account the capacity and reliability;

   b. risks related to track record, business continuity, and financial balance of service provider;

   c. ensuring that the contractual terms and conditions regulating the role, relationship, obligations, and responsibilities of all parties are fully set out in an agreement that covers at least performance target, service level, availability, reliability, capacity, compliance, audit, security, disaster mitigation planning, disaster recovery capability, backup processing facility, and choice of law;

   d. ensuring that the Information Technology service provider is able to provide access to information to all parties determined by the Administrator as well as supervisory institution and sector regulator for arrangement, audit, or compliance; and

   e. capable of performing supervision and evaluation to the performance of activities of Administrator that are organized by the service provider periodically concerning performance, reputation of service provider, and continuity of service provision.

5. Administrator shall ensure the Information Technology service provider:

   a. has the expert staff that has reliability supported by certificate of competency academically and/or professionally in accordance with the need for organizing Information Technology;

   b. applies the principle of Information Technology control adequately as proven with the result of audit performed by independent party;

   c. as the affiliated party, maintains the security of all information including secret of Administrator and personal data of customer;

   d. reports to the Administrator every critical event that may cause significant financial loss and/or disrupting the smooth operational of Administrator;

   e. delivers the result of audit on Information Technology performed by independent auditor periodically to the Chief Executive Supervisor of Insurance, Pension Fund, Financing Institution, and Other Financial Service Institution through the corresponding Administrator;

   f. provides a tested and adequate Disaster Recovery Plan;

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.

g. complies with the clauses on early termination as set out in the agreement between Administrator and provider of Information Technology management transfer; and

h. complies with the service level in accordance with service level agreement between the Administrator and Information Technology service provider.

6. Administrator shall deliver the result of assessment for the application of risk management in the Information Technology service provider to the Chief Executive Supervisor of Insurance, Pension Fund, Financing Institution, and Other Financial Service Institution periodically every 3 (three) months at the latest on date 30.

7. In the event that date 30 as referred to in figure 6 falls on holiday, therefore, delivery shall be made at the latest of 1 (one) next business day.

8. Administrator shall ensure the destruction of data and information during the turnover of provider of Information Technology management transfer in accordance with this Circular Letter of OJK.

9. Administrator shall prepare report on use of management transfer and delivers it to the Chief Executive Supervisor of Insurance, Pension Fund, Financing Institution, and Other Financial Service Institution.

VI. MANAGEMENT OF DATA AND INFORMATION

1. Administrator shall be prohibited to disseminate personal data and information of User to other party.

2. Personal data and information of User as referred to in figure 1 shall include, at least:

a. data and information adhered and identifiable:

1) individual such as:

a. name;
b. domicile address;
c. identity card (*KTP, SIM*, Passport);
d. Taxpayer Identification Number (NPWP);
e. date of birth and/or age;
f. email address;
g. IP address;
h. telephone number;
i. account number;
j. name of biological mother;
k. credit card number;
l. digital identity (Biometric);
m. signature;
n. education history;
o. employment history;
p. checking account;

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.

q. list of assets;
r. other relevant data and information;

2) corporation:

a) name of corporation;
b) address;
c) telephone number;
d) structure of the board of directors and commissioner including identity document in the form of KTP/Passport/stay permit;
e) structure of shareholders;
f) account number;
g) checking account;
h) list of assets;
i) company documents;
j) other relevant data and information;

b. material non-public data and information:

1) financial statement;
2) business performance;
3) management decision;
4) number of subscribers;
5) other relevant data and information;

c. data and information related to financial transaction; and

d. data and information related to contract/agreement.

3. Prohibition as referred to in figure 1 shall be excepted in the event that:

a. User grants written approval; and/or
b. it is obligated by the applicable laws and regulations.

4. In the event that User grants written approval as referred to in figure 3 letter a, Administrator may provide personal data and/or information of User and ensures the contemplated third party does not provide and/or use the personal data and/or information of User for the purpose of other than as agreed upon between the Administrator and other party.

5. Procedures for written approval from User may be declared, among others, in the form of:

a. agree or disagree option; or
b. providing approval sign,

in the document and/or agreement of products and/or services.

6. Data and information as referred to in figure 2 must be secured using the method that can ensure the data reading process is performed by the authorized party.

7. Data and information of User that is obtained and utilized by Administrator must meet the following criteria:

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.

a. delivery of limitation of utilization of data and information to User as well as acquiring approval from User;

b. delivery of every change of objective of utilization of data and information to User (if any); and

c. media and method used in acquiring data and information is guaranteed the confidentiality, security as well as the integrity.

8. Data or information of User that is destroyed by Administrator must meet the following criteria:

a. take into account the retention aspect based on the applicable laws and regulations and audit interests as well as audit from the supervisory authority and sector regulator; and

b. ensure there is no data and information left behind, correlated and can be reused.

9. Administrator shall prevent the existence of invalid access to the data and information.

10. Administrator shall be obligated to maintain the confidentiality, integrity, and availability of personal data, transaction data, and financial data that it manages as from the data is acquired up to the data is destroyed.

VII. INFORMATION TECHNOLOGY RISK MANAGEMENT

1. Administrator must perform risk identification, assessment, and mitigation, at least, with regard to the:

a. assets owned;
b. process business performed;
c. classification of data and information;
d. caretaker of risk;
e. acceptable risk limit; and
f. determination of impact assessment and possible occurrence of risk.

2. Administrator shall determine the risk tolerance becoming the reference to the risk management.

3. Administrator must identify the possible occurrence of deficiencies and/or defects in Electronic System as from the design, development, and operation stages to anticipate failure in Electronic System.

4. To ensure the Electronic System risks are well-measured and controlled, therefore, Administrator shall determine the framework of Information Technology risk management.

5. Administrator shall perform periodic update and monitoring risk analysis to ensure every change in Electronic System, Information Technology infrastructures, or Information Technology operational is identifiable.

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.

VIII. ELECTRONIC SYSTEM SECURITY

Administrator shall ensure the Electronic System security is performed effectively and continuously by taking into account the following matters:

1. Administrator must prepare, determine, and socialize the policies, procedures, and standards of Electronic System security continuously;

2. Electronic System security must meet the elements of confidentiality, integrity, and availability;

3. Electronic System security must take into account the aspects of technology, human resources, and utilization of Information Technology;

4. Electronic System security that is applied must be based on the result of risk assessment;

5. availability of management on handling incident in Electronic System security.

6. monitoring, assessment, and handling the security gap of Information Technology routinely and periodically to the Electronic System that supports the business processes of Administrator by taking into account risk management;

7. Administrator shall ensure that the access to data and information by internal as well as external parties meet the prudential principle and limited access principle.

IX. HANDLING INCIDENT AND SURVIVAL TO THE INTERFERENCE

In the case of handling incident and survival to the interference, Administrator shall:

1. ensure the procedures of handling incident and survival to the occurred interference, at least, covering:

    a. classification of incident;
    b. measures of handling incident;
    c. recording of incident; and
    d. database of problems and incident;

2. prepare and test periodically the plan and specific measure required to be taken when an incident is able to provide significant impact to the operational or business of Administrator;

3. have the planning and method to deliver information regarding interference to the relevant external party to be able to settle the occurred incident and/or interference;

4. have the planning and method to communicate the occurred incident or interference if such matter has impact to subscriber or other stakeholder;

5. provide the procedures and media for User to submit complaint(s) regarding the services rendered by the Administrator;

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.

6. provide the method of backup information delivery that is separated and different from the Electronic System used for the operational to anticipate disaster event.

X. USE OF ELECTRONIC SIGNATURE

1. The Information Technology-Based Money Lending Services Agreement that is signed using Electronic Signature shall have equal legal force and legal consequences with the agreement signed using wet ink.

2. Administrator must have employees that are responsible to manage the fulfillment of Information Technology-Based Money Lending Services agreement by using Electronic Signature.

3. In the framework of using Electronic Signature, Administrator shall cooperate with the Administrator of Electronic Signature.

4. Administrator of Electronic Signature as referred to in figure 3 shall meet, at least, the following qualifications:

   a. registered at the Ministry of Communication and Informatics of the Republic of Indonesia;

   b. has security standard and Information Technology in accordance with the applicable laws and regulations;

   c. submits periodic report regarding the performance and outcome(s) of audit to the Administrator;

   d. has the capability to secure data of Administrator and User using encryption method and apply the principle of minimum access right;

   e. has the method to issue, delete, and replace Electronic Certificate at the request of the respective Administrator or User;

   f. has the method to perform verification to the Electronic Signature that has been affixed as well as the issued Electronic Certificate;

   g. able to perform time tagging process for each process of electronic signing; and

   h. able to perform the process of revocation and re-issuance of problematic Electronic Certificate at the request of the respective Administrator or User.

5. Qualification as referred to in figure 4 letter b up to letter h shall be proven with the outcome(s) of audit on Information Technology that is performed by credible independent auditor and has international reputation.

6. Chief Executive Supervisor of Insurance, Pension Fund, Financing Institution, and Other Financial Service Institution shall grant approval for the performance of cooperation between the Administrator and Administrator of Electronic Signature as referred to in figure 3.

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.

7. In the event of utilization of Electronic Signature, Administrator shall take into account, at least, the followings:

   a. integration process between the Electronic System of Administrator with Administrator of Electronic Signature must be able to maintain the authenticity of identities of the parties performing the Electronic Transaction;

   b. integration process between Electronic System of Administrator and Administrator of Electronic Signature shall ensure the security and governance aspects owned by the Administrator are constantly maintained;

   c. process of Electronic Transaction data processing, storage, as well as utilization must take into account the principle of integrity of the Electronic Transaction to be always maintained; and

   d. delivers the rights and responsibilities of User having and utilizing Electronic Signature.

XI. AVAILABILITY OF SERVICES AND TRANSACTION FAILURE

1. Administrator shall define and execute the procedures and facilities for the Electronic System security in avoiding interference, failure, and loss.

2. Administrator shall provide security system that covers procedures, prevention and mitigation system to threats and attacks causing interference, failure, and loss.

3. In the occurrence of system failure or interference with serious impact due to the acts of other party to the Electronic System, Administrator shall secure the data and report it to the Chief Executive Supervisor of Insurance, Pension Fund, Financing Institution, and Other Financial Service Institution as well as announce it to User at the latest of 1 (one) hour following the occurrence of system failure or interference.

4. Administrator shall have alternative communication channel to ensure the continuity of service to User.

5. Administrator must perform continuous monitoring and evaluation for the operational and service of Information Technology continues to run well.

XII. TRANSPARENCY OF INFORMATION OF PRODUCTS AND SERVICES

1. Administrator must include information of products and services in the Electronic System used by the Administrator.

2. Inclusion of information of products and services must take into account at least the followings:

   a. risks adhered to the products and services;

   b. basic description of products offered;

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.

c. complaint center; and/or

d. cost arising in relation to the products and services.

XIII. RETENTION

Administrator shall be obligated to re-display the overall data and information in accordance with the initial format by constantly taking into account the retention period based on the applicable provisions of laws and regulations.

XIV. CLOSING

Provisions in this Circular Letter of OJK shall come into effect as from the date of its stipulation.

Stipulated in Jakarta
on 18 April 2017

DEPUTY CHAIRPERSON OF THE BOARD OF COMMISSIONERS
FINANCIAL SERVICE AUTHORITY

sgd
RAHMAT WALUYANTO

Issued as a true copy
Director of Legal Affairs 1
Department of Legal Affairs

sgd
Yuliana

NOTE

Source: LOOSE LEAF OF CIRCULAR LETTER OF DEPUTY CHAIRPERSON OF THE BOARD OF COMMISSIONERS OF FINANCIAL SERVICE AUTHORITY YEAR 2017

Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.
Copyright © 1997 - 2017 PT Legal Centric Indonesia. All Rights Reserved.