ACTIO

ISSUE NO. 9 / JANUARY 2019

What Is The Validity of Electronic Signatures As a Means of Transaction in Indonesia?

Regulation and Implementation of Cyber Insurance

Financial Technology Supervision Mechanism

How To Deal with Fake News and Cyber Bullying

9 772528 280004

TABLE OF CONTENT

ACTIO

Editorial:
Supervisor:
Setyawati Fitri Anggraeni, S.H., LL.M.,FCIArb., FAIADR.
Editor-in-chief:
Imelda Napitupulu, S.H., M.H.
Executive Director:
M. Adhima Djawahir, S.H.
Writers:
Dr. Hary Elias, BA Hons (Cantab), LL.M (1st Class Hons), MBA (Columbia), Juris Doctor
Keshia Bucha, S.H.
Wenny Novia, S.H.
David Gayus El Harun Marpaung, S.H., MKn.
Sechabudin, S.H.
Tubagus Kudrat Kun, S.H.
Contributor:
Media Consultant:
Fifi Juliana Jelita
Script Editor:
Wahyu Hardjanto
Visual Stylist:
Riesma Pawestri
Illustration: **freepik.com**

Axio Magazine is published every four months, made and distributed by:

ANGGRAENI and Partners

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace."

-Newton Lee-

Dear readers,
We hope you are blessed with good health while reading this 9th Edition of ACTIO

Over the past few years, various technological advancements have made things more accessible and convenient for us. Information is easily received and distributed. Consequently, this may be exploited by irresponsible parties to conduct harmful deeds. For example, publishing fake news that result in the emergence of "cyber risk" or chaos that occurs due to failure of the human element in technology and information systems.

Therefore, responsibility for mitigating cyber risk does not only belong to the IT team but to all layers within an organization.

In order to raise the awareness to the threat of cybercrime, ACTIO 9th Edition decided to pick up the theme of "Cyber Risk". Our coverage of the topic include a wide array of aspects, starting from how to respond to fake news (hoax) and cyber bullying, legal protection for victims of personal data breach, development of cyber insurance, discussion of PERMEN KOMINFO No.11 of 2018, and legal protection for application users against the e-commerce technology business empire and the mechanism of financial technology supervision.

Lastly, all of us from ACTIO Team wish our dearest readers happy reading and may you find this edition particularly useful to you.

Happy New Year 2019 and we wish you all Season's Greetings and a profitable year ahead.

Warmest regards,
Setyawati Fitri A, S.H., LL.M., FCIArb., FAIADR.

CONSEQUENCES OF FAKE NEWS AND CYBER BULLYING

The advancement of technology is affecting all aspects of social activity including the ease in receiving and disseminating information. However, the ease in receiving and disseminating information provides an opportunity for some parties to publish fake news or to bully others to create chaos in society.

Spreading fake news and cyber bullying is clearly to be avoided as the speed with which fake news is spread can have wide scale repurcussions. Tackling the circulation of fake news and cyber bullying in the community can be conducted through increasing the awareness of the community regarding the consequences received by the perpetrators who publish fake news and cyber bullying.

Law Number 11 of 2008 as amended by Law Number 19 of 2016 concerning Electronic Information and Transactions ("Law 19/2016") penalizes a person, who intentionally and without authorization disseminates false and misleading information resulting in consumer loss in electronic transactions,[1] to a sentence of up to imprisonment of 6 (six) years and/or a fine of up to Rp 1.000.000.000 (one billion Rupiah).[2]

With respect to cyber bullying, a perpetrator who intentionally and without authorization sends electronic information and/or electronic records that contain violation threats or intimidation against individuals shall be sentenced to imprisonment of up to 4 (four) years and/or a fine of up to Rp 750.000.000 (seven hundred fifty million Rupiah).[3]

These are severe penalties aimed at discouraging the abuse of electronic messages and it is desirable that encouraging public awareness regarding the consequences of spreading fake news and cyber bullying is important. This will hopefully deter fake news and cyber bullying with the hope that people use technology more responsibly. **MAD/HES**

1. Electronic transaction is a legal action conducted with computer, computer network and/or other electronic media; **2.** Article 45 A paragraph (1), Law 19/2016; **3.** Article 45 B, Law 19/2016.

REGULATION NUMBER 11 OF 2018

CONCERNING THE IMPLEMENTATION OF ELECTRONIC CERTIFICATION

Along with the development of electronic transactions, electronic signatures and electronic certificates have a very important role that needs to be regulated specifically. This year, Indonesia has regulated the implementation of electronic certification with the issuance of the Republic of Indonesia Minister of Communication and Information Technology Regulation Number 11 of 2018 concerning the Implementation of Electronic Certification on September 6, 2018 ("Regulation No. 11/2018").

An Electronic Certificate in an electronic transaction is the approval of the owner of the Electronic Certificate for information and / or electronic documents signed with the Electronic Certificate.[1] Electronic certificates are issued, extended, revoked and blocked by an institution called Electronic Certificate Provider[2] in the form of a legal entity.[3] There are 3 types of Electronic Certificate Providers, namely (i) a registered Electronic Certification Provider; (ii) a certified Electronic Certification Provider; or (iii) an entity holding Electronic Certification Provider.[4]

Electronic Certification Providers are generally obliged to (i) organize the administrative processes; (ii) verify the applicant's identity; (iii) extend the validity period of the Electronic Certificate; and (iv) create an active and passive database of Electronic Certificates and maintain records that can be accounted for in both written (paper based) and electronic (electronic based) forms (v) maintain the confidentiality of the identity of the Electronic Certificate Owner from an unauthorized party; (vi) notify the Electronic Certificate Policy to the prospective owner of the Electronic Certificate and the Owner of the Electronic Certificate issued by them.[5]

Applicants who submit applications to obtain admission as Electronic Certification Provider must fulfill the requirements by attaching documents in accordance with the level of recognition status of the Electronic Certification Provider requested (registered provider/ certified provider/ holding provider).[6] After passing verification, the applicant will obtain admission as an Electronic Certification Provider in accordance with the level of admission status that is valid for 3 (three) years.[7]

Electronic Certification Providers who have received admission will be included in the list of Electronic Certification Provider and published on the Ministry of Communication and Information Technology's webpage.[8] Thus, the issuance of this regulation and the information disclosure are expected to be able to provide benefits to the industry and public. **KBA/HES**

---

1. Article 26 paragraph (2) Regulation of the Minister of Communication and Information No. 11/2018; **2.** Article 25 paragraph 1 jo. Article 25 paragraph 2 Regulation of the Minister of Communication and Information No. 11/2018; **3.** Article 1 number 6 Regulation of the Minister of Communication and Information No. 11/2018; **4.** Article 5 Regulation of the Minister of Communication and Information No. 11/2018; **5.** Article 21 Regulation of the Minister of Communication and Information No. 11/2018; **6.** Article 13 paragraph (1) Regulation of the Minister of Communication and Information No. 11/2018 jo. Article 5 Regulation of the Minister of Communication and Information No. 11/2018; **7.** Article 14 paragraph (1) Regulation of the Minister of Communication and Information No. 11/2018; **8.** Article 15 paragraph (1) jo. Article 15 paragraph (2) Regulation of the Minister of Communication and Information No. 11/2018.

REGULATION AND IMPLEMENTATION OF CYBER INSURANCE

Law Number 40 Year 2014 concerning Insurance and its implementing regulation do not specifically define the meaning of cyber insurance. However, in short, cyber insurance may be defined as insurance providing protection over risks occurred to computer system and data. Based on its character, cyber insurance may be classified as a part of general insurance, namely a business of insurance service providing a compensation to the insured or policy holder due to loss, damage, incurred cost, profit loss, or legal liability towards third parties which may be suffered by the insured or policy holder due to an uncertain event.

The main object of cyber insurance is protection over software and data. Risks secured by cyber insurance cover (i) risk on business disruption as a result of cyber-attack, (ii) computer fraud, (iii) protection over data privacy regulation and fine, (iv) cyber blackmail, and (v) loss of digital assets.

The number of insurance companies providing cyber insurance service in Indonesia is still very low and only dominated by international top tier insurance companies. Pursuant to information from the Executive Director of General Insurance Association of Indonesia (Asosiasi Asuransi Umum Indonesia - AAUI), until 2017, no more than 10 insurance companies provide such cyber insurance. The Insurance companies providing such cyber insurance include inter alia PT Asuransi Tokio Marine Indonesia, PT AIG Insurance Indonesia, dan PT Chubb General Insurance Indonesia. **SCN/HES**

PEER-TO-PEER (P2P) LENDING SERVICE IN INDONESIA: AN OVERVIEW

Peer-to-peer lending platforms, offering loans ranging from as little as few thousand rupiah to several million rupiah, have so far been welcomed by Indonesia. Although Southeast Asia's biggest economy, Indonesia is a country where tens of millions of people have little or no access to bank credit. This gap in loan needs and credit is fertile ground for the popularity of P2P lending platforms.

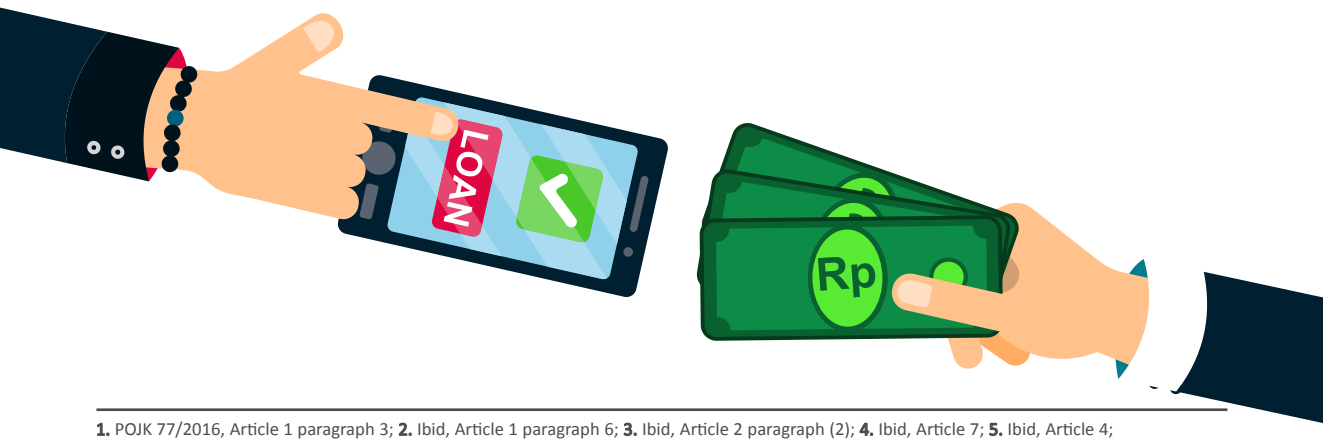
On December 2016, the Financial Services Authority ("OJK") enacted OJK Regulation No. 77/POJK.01/2016 regarding IT Based Lending Services ("POJK 77/2016"). This POJK 77 2016 introduces various guidelines, obligations and restrictions in an attempt to establish a framework for P2P businesses.

A P2P Lending Service is defined as financial services provided via an online platform that matches lenders and borrowers to facilitate entry into loan arrangements by an electronic system through the internet facility.[1] Also, a P2P Lending Service Provider ("Provider") is an Indonesian legal entity that provides, maintains and operates the P2P Lending Services.[2]

Under POJK 77/2016, Providers specifically exclude other financial institute on. A Legal entity as mentioned above for the purposes of a Provider shall either be a limited liability company ("PT") or cooperative ("Koperasi").[3]

POJK 77/2016, stipulates 2 (two) stages before a Provider can do business. First, the registration stage and second the business license stage.[4] The registration certificate and business licenses are issued by OJK. Any PT Provider who wishes to obtain a registration certificate must have a paid-up capital at least IDR 1 Billion, and must increase its paid up capital to at least IDR 2.5 Billion by the time the PT Provider applies for a business license. A Koperasi Provider is subject to the same capital requirements for its equity at the registration and business license stage.[5]

77/2017 stipulates also requires specific qualifications for the employees and management of the Provider. Employees must have IT background or expertise and at least one director and commissioner must have a minimum 1 (one) year's expertise and experience in the financial services industry.[6] A further specific pre-qualification is for data center and disaster recovery center to be located in Indonesia.[7] **TKK/HES**



1. POJK 77/2016, Article 1 paragraph 3; **2.** Ibid, Article 1 paragraph 6; **3.** Ibid, Article 2 paragraph (2); **4.** Ibid, Article 7; **5.** Ibid, Article 4; **6.** Ibid, Article 14; **7.** Ibid, Article 25.

ELECTRONIC INFORMATION AND ELECTRONIC DOCUMENT AS EVIDENCE UNDER PENAL LAW

Technological advances in people's lives provide convenience for users to carry out daily activities. The convenience provided by technological advances can be seen in various aspects, one of which is the legal aspect. The presence of electronic information and/or electronic documents can be used as evidence and proof that an event has occurred. However, until now there is still a debate on the admissibility of electronic information and/or electronic documents as evidence in the trial.

Article 184 of the Criminal Procedure Code stipulates that legal evidence includes (i) witness statement, (ii) expert statement, (iii) letter, (iv) instructions and (v) statement of the defendant. As explained in the provisions of the article above, Article 184 of the Criminal Procedure Code has expressly limits as to the types of evidence that can be used as proof at the trial. [1]

Furthermore, Article 5 of Law Number 11 of 2008 as amended by Law Number 19 of 2016 concerning Electronic Information and Transactions ("Law 19/2016") stipulates that electronic information and/or electronic documents and/or printed results is legitimate legal evidence[2] and is an extension of legal evidence in accordance with the applicable Laws in Indonesia.[3] Referring to the provisions of Article 5 of Law 19/2016, informed that in criminal proceedings, electronic information and/or electronic documents can be used as legal evidence.

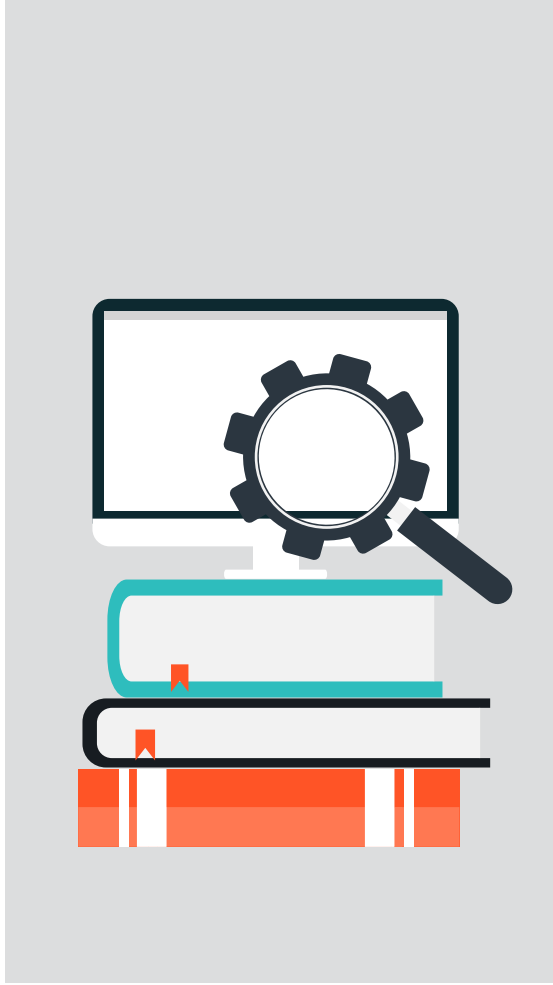
In the Supreme Court Decision Number: 777/Pid.B/2016/PN.JKT.PST in the case of Jessica Kumala, the Public Prosecutor used the CCTV record results as evidence, for consideration by the Judge explaining that CCTV footage can be used as an extension of Article 184 paragraph (1) of the Criminal Procedure Code as evidence if it corresponds to criminal facts and events, so that it can be used by the Panel of Judges as guidance. However the use of electronic evidence as legitimate evidence is being limited as stated in Indonesia's Constitutional Court Decision Number 20/PUU-

1. https://www.kejaksaan.go.id/unit_kejaksaan.php?idu=28&idsu=35&id=4183, accessed on 7 December 2018; **2.** Article 5 paragraph (1), Law 19/2016; **3.** Article 5 paragraph (2), Law 19/2016.

XIV/2016 submitted by Drs. Setya Novanto. In its consideration, the Court stated that to prevent differences in interpretation of Article 5 paragraph (1) and paragraph (2) of Law 19/2016 it must be emphasized that each interception shall be conducted legally, especially in the context of law enforcement by adding the word or phrase "specifically".[4]

Based on the decisions above the Judge's consideration as stated in Supreme Court Decision Number: 777/Pid.B/2016/PN.JKT.PST is correct. That the CCTV used as evidence is in accordance with the criminal event. The presence of technological ability to record and store data may be used as evidence for the Judges' consideration. This is notwithstanding that Article 188 paragraph (2) of the Criminal Procedure Code states that the instructions can only be obtained through (i) witness statements, (ii) letters and (iii) defendant's information. However, if electronic information and/or electronic documents can help Judges to have a better understanding of the evidence and therefore able to come to a more correct and fair verdict, then , electronic information and/or electronic documents should normatively be admissable as valid evidence.

Dr. Edmon Makarim, S.Kom, S.H, LL.M said in the Indonesia's Constitutional Court Decision Number 20/PUU-XIV/2016 that there must be a separation between the evidence and the process to obtain the evidence, so that all electronic information and/or electronic documents and/or printed results is a legal proof of law.[5] Based on the Indonesia's Constitutional Court Decision Number 20/PUU-XIV/2016 the judges agreed with Dr. Edmon Makarim, S.Kom, S.H, LL.M proposition that clearer regulations must be passed regarding the procedures for obtaining electronic



information and/or electronic documents to ensure the accuracy and validity of the electronic evidence. By its nature, electronic evidence is easily manipulated and corrupted. Thus, stricter rules of evidence need to be in place to ensure the chain of evidence and perhaps the downloading and safe keeping process of such electronic evidence.

In the final analysis, electronic information and/or electronic documents are legitimate evidence and are admissable under the penal law so long as the method used to obtain the electronic information and/or electronic documents is in accordance with the applicable laws and regulations. **ADP/MAD/HES**

4. Supreme Court Decision Number: 777/Pid.B/2016/PN.JKT.PST, page 96;
5. Indonesia's Constitutional Court Decision Number 20/PUU-XIV/2016, page 106.

Q: What Is The Validity of Electronic Signatures ("TTE") As a Means of Transaction in Indonesia?

A: First of all, we should know what is the definition of "signature" according to Indonesia Dictionary ("KBBI") is "a sign as a symbol of the name written by hand by the person himself as a personal sign (has received)."

Further, "Electronic Information" means "one cluster or clusters of electronic data,[1] including but not limited to writings, sounds, images, maps, drafts, photographs, electronic data interchange (EDI), electronics mails, telegrams, telex, telecopy or the like, letters, signs, figures, Access Codes, symbols or perforations that have been processed for meaning or understandable to persons qualified to understand them." So, "Electronic Signature" means "a signature that contains Electronic Information that is attached to, associated or linked with other Electronic Information that is used for means of verification and authentication."

The updated regulation Law No. 19 of 2016 ("Amendment") on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("2008 EIT Law"), Amendment took effect on 25 November 2016 does not amends the previous regulation regarding the validity of the TTE. Amendment has more concern on privacy protection, meaning of Electronic System Provider ("ESP") and government right to terminate access or order an ESP to terminate access.

So, in addressing whether TTE has legal consequences will be explained the conditions in written under Article 11 2008 EIT Law:

(1) TTE/Electronic Signatures shall have lawful legal force and legal effect to the extent satisfying the following requirements:

a. Electronic Signature-creation data shall be associated only with the Signatories/Signers;
b. Electronic Signature-creation data at the time the electronic signing process shall be only in the power of the Signatories/Signers;
c. Any alteration in Electronic Signatures that occur after the signing time is knowable;
d. Any alteration in Electronic Information associated with the Electronic Signatures after the signing time is knowable;
e. There are certain methods adopted to identify the identity of the Signatories/Signers; and
f. There are certain methods to demonstrate that the Signatories/Signers have given consent to the associated Electronic Information;

Elucidation of Article 11 Section (1):[2]
This Law grants recognition definitely that despite codes, TTE/Electronic Signatures have an equal position to manual signatures in general, with legal force and legal effect.

The requirements as intended by this Article shall be the requirements that minimally any TTE/Electronic Signature must satisfy.
(1) Further provisions on Electronic Signatures as intended by section (1) shall be regulated by Government Regulation.

Elucidation of Article 11 Section (2):
The Government Regulation concerned shall govern, inter alia, techniques, methods, means or process for creating TTE/Electronic Signatures.

TTE/Electronic Signature further regulated specifically on **GR No. 82 of 2012** on Management System and Electronic Transaction on Chapter V from **Article 52 till 58**. Furthermore, this GR has classified the TTE/Electronic Signature into Certified TTE and Non-Certified TTE.[3]

In connection with the security and convenience of online transactions and transactions in general that requires TTE, we recommend in using a certified TTE to prevent the risk of forgery or misuse of your signature. **RKT/HES**

1. Great Indonesian Language Dictionary; **2.** Law No. 11 of 2008 concerning Electronic Information and Transactions; **3.** PP No. 82 of 2012 concerning the Implementation of Systems and Electronic Transactions.

LEGAL REMEDIES FOR BREACH OF CONFIDENTIALITY OF PERSONAL DATA

Because of the advancement of technology, it has become the norm for developers to compete with each other to release applications which provide cross services ranging from social media, marketplace, tourism, finance and etc. These applications generally offer a variety of services aimed at providing convenience at a low cost or even at zero cost in order to appeal to the masses. In order to improve and run the provided services, more often than not, the developers need to harvest the user's personal data. In fact, it has become common practice for developers to require that users must grant their consent to developers to use their personal data before they are granted access to the said applications. Thus, the larger the database of users of an application, the greater the amount of personal data coming under the control of the developer of the application. In essence, application developers now act as data controllers or data processors.

Considering the vast amount of personal data, it is reasonably expected of data controller to protect the data with utmost responsibility and care. However, in reality, breach of personal data is a common occurrence and happens whenever personal data is being released intentionally or unintentionally. One of the biggest cases of personal data breach that successfully grabbed the world's attention recently was the leak of 50 (fifty) million Facebook users to Cambridge Analytica, a political data analysis consulting firm based in the UK. Cambridge Analytica was able to unlawfully process the data of Facebook users due to Facebook's negligence which allowed third-party applications to obtain the users' personal data and use the data without the consent of the user or for purposes not consented for.

This high profile case further emphasizes the urgency and need for regulations that

provide options of legal remedies, including to injunctive relief, damages suffered by the owner of personal data whose personal data is being compromised and other remedies available. This will go a long way to ensure the public that the data controller/data processor will take all the necessary precautions to prevent a data breach on the pain of penalties. In Indonesia, the draft national law on the protection of personal data is still under discussion at the legislative level. There is yet no comprehensive law that specifically governs data protection. Provisions on protection of personal data are still uncentralised and are found in various laws and regulations.

Article 26 paragraph 1 of Law No. 11 of 2008 as amended by Law No. 19 of 2016 ("ITE Law") for example, stated that unless stipulated otherwise by law, the use of any information through electronic media relating to one's personal data must be carried out with the consent of the person concerned. If this provision is violated, then any person whose rights have been violated are entitled to file a claim for damages against those who are using their personal data without consent.

In addition to the ITE Law, provisions on personal data protection are also regulated under the Minister of Information and Communication Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems ("Perkominfo 20/2016"). Under this regulation, besides filing a claim for damages, the owners of personal data are also entitled to file a complaint to the Minister of Communication and Information that the data processor/data controller has failed to protect the confidentiality of their personal data and that the organizer of the system does not provide written notice to the owner of the data or late in giving written notice while losses have occurred. These complaints shall be resolved by deliberation or through the means of alternative dispute resolutions.

Last but not least, the government may impose the following administrative sanctions on anyone who is accountable for the misuse of personal data including :

a. Oral warning
b. Written warning
c. Termination of activities; and / or
d. Announcements on sites on the network.

In conclusion, the legal remedies for breach of confidentiality of data consists of claims and complaints. However, the current legal regulations in Indonesia concerning personal data protection still leave a lot to be desired. For example, the current regulations have not stipulated provisions regarding the implementation of the aforementioned legal remedies against data controllers/processors that are domiciled overseas. This is especially important as many data controllers/processors are foreign entities. Thus, it is hoped that the Government will complete the draft law on the protection of personal data soon in order to protect the legal interests of the nation and the people of Indonesia. **WNA/HES**

THE REGULATION OF DATA CENTER IN INDONESIA

Electronic System Providers guarantee that every component and integration of all Electronic Systems operate properly. Electronic System Components include Hardware, Software, Experts, governance, and security. Government Regulation of the Republic of Indonesia Number 82 of 2012 concerning the Implementation of Electronic System and Transactions ("PP 82/2012") regulates the obligations of Electronic System Providers in general and Electronic System Providers for public services.

Electronic System Providers for public services, among others, are required to provideg a data center and disaster recovery center in the territory of Indonesia, and must obtain an Electronic System Feasibility Certification from the Minister, and must be registered with the ministry that organizes government affairs in the field of communication and informatics.

Q: What is a Data Center?

A: A Data Center is a facility used to place computer systems and related components, such as telecommunications systems and data storage for the purposes of data placement, storage and processing.

Q: What is the role of the government in using Data Centers?

A: Based on the Regulations of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Regulations Number 11 of 2008 concerning Information and Electronic Transactions ("Regulations 19/2016"), explains that the Government facilitates the use of Information Technology and Electronic Transactions and has the duty to protect the public interest from all types of disturbances as a result of misuse of Electronic Information and Electronic Transactions that disrupt public order.

The government must establish institutions that have strategic electronic data that must be protected which are then required to make Electronic Documents and electronic backup records and connect them to certain data centers for the benefit of data security.

Q: What is the purpose of the Data Center?

A:

- Provide security, justice and legal certainty for data center managers and users;
- Protect the public interest from misuse and risk of loss due to management and use of data centers that are not in accordance with the provisions of legislation;
- Provide convenience for the community in obtaining and using data centers;
- Providing protection and enforcement of statehood towards the data of its citizens.

DGM/HES

1. Explanation of Article 17 paragraph (2) PP 82/2012; **2.** Article 40 paragraph (4) of Law 19/2016.

FINANCIAL TECHNOLOGY SUPERVISION MECHANISM IN INDONESIA

The Financial Technology ("Fintech") industry is mainly regulated by 3 (three) administrative bodies; the Central Bank of Indonesia (BI), Financial Services Authority (OJK), and the Ministry of Communication and Informatics (Kemenkominfo). BI and OJK are responsible for different segments of the fintech industry. Fintechs that offer payment systems are regulated under BI. Other sectors such as lending, crowdfunding, insurance, etc, fall under the governance of OJK. Supporting the technological aspects of the industry, Kemenkominfo regulates the framework for data protection, data centers and IT infrastructure.

OJK has released regulation for fintech development and has established a regulatory framework[1] through OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovation in the Financial Services Sector ("POJK 13/2018"). POJK 13/2018 defines Digital Financial Innovation as "any form of innovation in business processes, business models or financial instruments that provide added value in the financial services sector through participation in a digital ecosystem.",[2] which provides a variety of fintech services, such as:[3]

- Transactional settlements;
- Capital accumulation;
- Investment management;
- Fund accumulation and distribution;
- Insurance;
- Market support;
- Other digital supporting services; and/or
- Other financial services operations.

BI has also added regulations with respect to the payment sector in Regulation of Bank Indonesia No. 19/12/PBI/2017 on the Application of Financial Technology. In these regulations, 'regulatory sandbox' is defined as a testing mechanism conducted by the OJK or BI to assess business process reliability, business models, finance instruments, and governance of the Operator.

This "Regulatory sandbox" regime in BI and OJK are designed to evaluate the value of the innovation to the public. After completing the sandbox process, the OJK and/or BI (depending on the nature of the fintech) will issue a 'recommendation status' determination for the provider, stating either:[4][5][6]

- Recommended;
- Not recommended;
- Required to make improvements.

TKK/HES

1. Regulatory sandbox is a mechanism of testing carried out by the Financial Services Authority to assess the reliability of business processes, business models, financial instruments and administrators; **2.** Financial Services Authority Regulation No. 13 / POJK.02 / 2018, Article 1; **3.** Ibid., Article 3; **4.** Regulation of the Financial Services Authority, Op. Cit, Article 11 (1); **5.** Bank Indonesia Regulation No. 19/12 / PBI / 2017, Chapter IV concerning Regulatory Sandbox; **6.** Ibid, Article 12 (2).

ANGGRAENI AND Partners

www.ap-lawsolution.com

TENDEAN SQUARE KAV. 17-18
Jl. Wolter Monginsidi No. 122-124
Kebayoran Baru, South Jakarta
Indonesia – 12170

PHONE : +62-21-72787678, 72795001
FAX : +62-21-7234151
EMAIL : connect@ap-lawsolution.net