DENTONS HPRP

Grow | Protect | Operate | Finance

Summary and Implication of the Second Amendment of Law No. 11 of 2008 Concerning Electronic Information and Transactions

Prepared by:

Mika Isaac Kriyasa (Partner), and Rovi Fremi Raturandang (Associate)

Since the issuance of Law No. 11 of 2008 concerning Electronic Information and Transactions, as amended by Law No. 19 of 2016 ("**IT Law**"), there have been several technological advances that need to be regulated by the Indonesian Government in order to maintain a clean, ethical, productive, and just digital space in Indonesia.

Therefore, on 2 January 2024, the Indonesian Government enacted Law No. 1 of 2024 concerning the Second Amendment of Law No. 11 of 2008 Concerning Electronic Information and Transactions ("**Second Amendment of the IT Law**") to address the developments occurring in the world of technology.

This article attempts to summarize several important changes in the Second Amendment of the IT Law that should be noted by business entities and the general public alike.

Legal Entity Forms for Electronic Certification Providers

The Second Amendment of the IT Law makes changes to the provisions regarding the legal entity forms of Electronic Certification Providers. The IT Law stated that Electronic Certification Providers operating in Indonesia can take the form of Indonesian or foreign Electronic Certification Providers. However, in the Second Amendment of the IT Law, Electronic Certification Providers operating in Indonesia must have a legal entity in Indonesia and be domiciled in Indonesia, except in cases where services using Electronic Certificates are not yet available in Indonesia.[1]

Therefore, since the issuance of the Second Amendment of the IT Law, foreign Electronic Certification Providers that are operating or will operate in Indonesia must adjust themselves by establishing a legal entity in Indonesia.

Further, the Second Amendment of the IT Law provides clearer regulations on the business activities of Electronic Certification Providers in accordance with the previously issued Ministerial Regulation.

The business activities of an Electronic Certification Provider include providing services such as:

a. Electronic signatures;
b. Electronic seals;
c. Electronic timestamps;
d. Recorded electronic delivery services;
e. Website authentication;
f. Preservation of Electronic Signatures and/or electronic seals;
g. Digital identities; and/or
h. Other services using Electronic Certificates.[2]

Mutual Recognition of Cross-Border Electronic Certificates

When the Second Amendment of the IT Law came into effect, the Indonesian Government thereby recognized the existence of cross-border Electronic Certificates. Mutual recognition for acknowledging cross-border Electronic Certificates is based on cooperation agreements, including agreements between Electronic Certification Providers or between Governments whose Electronic Certification Providers will reciprocally recognize each other, whether on a bilateral or multilateral basis.

[1]Article 13 paragraph (3) and (4) of Second Amendment of the IT Law.
[2]Article 13A paragraph (1) of Second Amendment of the IT Law.

As a result, documents or electronic transactions using cross-border Electronic Certificates can be acknowledged by the Indonesian Government, provided that the Electronic Certificates are based on a cooperation agreement between a legally established foreign Electronic Certification Provider and an Indonesian-based Electronic Certification Provider.[3]

The Utilization of Indonesian Law and Indonesian Language in International Electronic Contracts

The Second Amendment of the IT Law introduces a new provision that specifically relates to electronic contracts. The goal is to protect the Indonesian users of Electronic System Providers through the provision of guaranteed access to an effective and efficient legal system that will ensure the rights and obligations of Indonesian users and also dispute resolution.

International electronic contracts that are drafted by Electronic System Providers with standard clauses are now regulated under Indonesian law under the following conditions:

a. The Electronic System Provider service user, as one of the contracting parties in the electronic transaction, must originate from Indonesia and provide approval from or within Indonesian jurisdiction;
b. The implementation of the contract , including services, products, or electronic systems provided by the Electronic System Provider which are being utilized or accessed by Indonesian users, must be located within Indonesian territory; and/or
c. The Electronic System Provider has a business area (including a representative office) or conducts business activities within Indonesian territory.[4]

With the above being said, foreign Electronic System Providers cannot impose or substitute laws outside Indonesia as the governing law if any of the conditions mentioned above has been fulfilled.

Furthermore, the new provision also states that international electronic contracts should use Indonesian language that is concise, clear, and easy to understand, while also upholding principles of good faith and transparency.

Therefore, foreign Electronic System Providers must make adjustments to the governing law and language used in their international electronic contracts with parties in Indonesia.

Addition of Prohibited Acts Clause

The Second Amendment of the IT Law makes several adjustments to clauses related to prohibited acts. The specific adjustments are explained below:

No	Prohibited Action	Explanation	Sanctions	Implications
1.	Impugning the honour or good name of another person.	Any person or legal entity who intentionally impugns the honour or good name of another person by making accusations, with the intention of making such matters known publicly through Electronic Information and/or Electronic Documents conducted through an Electronic System.[5]	Maximum imprisonment of 2 years and/or maximum fine of Rp400,000,000.[6]	This provision is an adjustment to the regulations concerning defamation and slander that were previously stipulated in the IT Law. It explicitly outlines that impugning the honour or good name involves actions that degrade or damage the reputation or self-worth of others to their detriment, including defamation and/or slander.[7] One important consideration regarding this provision is particularly relevant when using social media. If social media users are not judicious in their comments, leading someone to feel that their self-worth is diminished or their reputation tarnished, then the affected individual can use this provision to pursue legal action against the person making such comments.
	The exemptions to this provision is if the action is: ***a. Conducted for the public interest; or*** ***b. Conducted as a form of self-defence.[8]***			

[3]Article 13 paragraph (5) and its Elucidation of Second Amendment of the IT Law.
[4]Article 18A paragraph (1) and its Elucidation of Second Amendment of the IT Law.
[5]Article 27A of Second Amendment of the IT Law.
[6]Article 45 paragraph (4) of Second Amendment of the IT Law.
[7]Elucidation of Article 27A of Second Amendment of the IT Law.
[8]Article 45 paragraph (7) of Second Amendment of the IT Law.

No	Prohibited Action	Explanation	Sanctions	Implications
2.	Threatening with violence.	Any person or legal entity intentionally and without right broadcasting, and/or transmitting Electronic Information and/or Electronic Documents, with the intent to unlawfully benefit themselves or others, to compel a person through violent threats to: a. provide an item, whether partially or entirely owned by that person or someone else; or b. incur a debt, make an acknowledgment of debt, or waive a claim.[9]	Maximum imprisonment of 6 years and/or maximum fine of Rp1,000,000,000.[10]	The provisions should minimize any threats of violence that are made by debt collectors in relation to a borrower and dissuade the lender from handing over a borrower's private data to debt collectors for them to threaten the borrower in relation to the repayment obligation.
3.	Threatening with defamation or disclosure of secrets.	Any person or legal entity intentionally and without right distributing, and/or transmitting Electronic Information and/or Electronic Documents, with the intent to unlawfully benefit themselves or others, to use threats of defamation or disclosure of secrets to compel a person to: a. provide an item, whether partially or entirely owned by that person or someone else; or b. incur a debt, make an acknowledgment of debt, or waive a claim.[11]	Maximum imprisonment of 6 years and/or maximum fine of Rp1,000,000,000.[12]	
4.	False notices or misleading information resulting in material losses for consumers.	Any person or legal entity intentionally distributing and/or transmitting Electronic Information and/or Electronic Documents containing false notices or misleading information resulting in material losses for consumers in Electronic Transactions.[13]	Maximum imprisonment of 6 years and/or maximum fine of Rp1,000,000,000.[14]	According to the previous IT Law, any consumer who suffers losses due to false news can press charges against any person or legal entity that disseminates such news. Nevertheless, in the Second Amendment of the IT Law, this provision does not apply to all consumer losses. Therefore, Consumers must, be able to prove that such losses are material.
5.	Hatred on race, nationality, ethnicity, skin colour, religion, belief, gender, mental disability, or physical disability.	Any person or legal entity intentionally and without right distributing and/or transmitting Electronic Information and/or Electronic Documents of a nature which incites, invites, or influences others in a way that creates hatred or hostility towards individuals and/or specific social groups based on race, nationality, ethnicity, skin colour, religion, belief, gender, mental disability, or physical disability.[15]	Maximum imprisonment of 6 years and/or maximum fine of Rp1,000,000,000.[16]	The Second Amendment of the IT Law includes not only hatred based on SARA (ethnicity, religion, race, and inter-group differences) but also adds hatred towards nationality, skin colour, beliefs, gender, mental disability, or physical disability. As we are aware, this year, Indonesia will hold Presidential and legislative elections. With the introduction of this provision, it is hoped that it can minimize the spread of hatred based on race, nationality, ethnicity, skin colour, religion, belief, gender, mental disability, or physical disability, especially in the context of undermining political opponents.

[9]Article 27B paragraph (1) of Second Amendment of the IT Law.
[10]Article 45 paragraph (8) of Second Amendment of the IT Law.
[11]Article 27B paragraph (2) of Second Amendment of the IT Law.
[12]Article 45 paragraph (10) of Second Amendment of the IT Law.
[13]Article 28 paragraph (1) of Second Amendment of the IT Law.
[14]Article 45A paragraph (1) of Second Amendment of the IT Law.
[15]Article 28 paragraph (2) of Second Amendment of the IT Law.
[16]Article 45A paragraph (2) of Second Amendment of the IT Law.

No	Prohibited Action	Explanation	Sanctions	Implications
6.	False notices causing public disturbance.	Any person or legal entity intentionally disseminating Electronic Information and/or Electronic Documents that they know contain false notices causing public disturbance.[17]	Maximum imprisonment of 6 years and/or maximum fine of Rp1,000,000,000.[18]	In the IT Law, there are no provisions specifically addressing false notices that cause public disturbance. However, the Second Amendment of the IT Law regulates this in order to maintain public order. Therefore, it is hoped that the public will exercise caution in disseminating news that may lead to public disturbances in physical spaces, not only in the digital realm.

[17]Article 28 paragraph (3) of Second Amendment of the IT Law.
[18]Article 45A paragraph (3) of Second Amendment of the IT Law.

- o0o -