



Client Alert March 2024

Navigating the New EIT Landscape: Understanding Key Changes under Law No. 1/2024

Law No. 1 of 2024, enacted on 2 January 2024, marks the second amendment to the Law No. 11 of 2008 regarding Electronic Information and Transactions initially established in 2008 (“EIT Law”). This revision aims to adapt to the rapid advancements in information and communication technology and enhance protection for Indonesian citizens within the digital world.

Overview

Law No. 1 of 2024 regarding Second Amendment to Law No. 11 of 2018 on Electronic Information and Transaction (“**Law No. 1/2024**”) introduces substantial changes for both individuals and businesses.

The amended law expands the scope of punishable digital offenses which resulted in varying penalties, enhancing electronic contracts and transactions, and social media misuse. Importantly, the amended law prioritizes public protection, strengthening safeguards, protecting children online, and fostering a secure and ethical digital environment for all users.

Key Changes and Observations

Law No. 1/2024 amended and/or added 27 (twenty-seven) articles from EIT Law. Below are the notable and salient point of changes made under the Law No. 1/2024:

Aspect	Before Amendment (EIT Law)	After Amendment (Law No. 1/2024)	Remarks
Electronic Certification Provider (“ECP”)	<ul style="list-style-type: none"> Foreign ECP operating in Indonesia must be registered in Indonesia. No specific scope of ECP services. 	<ul style="list-style-type: none"> Any ECP operating in Indonesia (including foreign) must be in the form of Indonesian legal entity and domiciled in Indonesia. ECP’s scope of services are regulated, including: (i) electronic signature; (ii) electronic seal; (iii) digital identity; and/or (iv) other services using electronic certificate. 	<p>Foreign ECP operating in Indonesia must now establish an Indonesian legal entity and domiciled within Indonesia. While this may create more equal environment for domestic and foreign ECPs, the transition process and any implications for existing foreign ECPs are yet to be clearly defined and regulated. On a side note, the explicit ECP’s scope of the core services brings more clarity to the business actors as well as regulatory control to the sector.</p>
Public Protection	<p>Limited provisions for specific group and general user protection.</p>	<ul style="list-style-type: none"> Introduced provision for child protection: Electronic System Provider (“ESP”) must ensure its product, services, and feature protects children’s rights. This is to be conducted by: (i) establishing minimum age restriction; (ii) child user verification; and (iii) reporting mechanism for content violation towards children’s rights. Expanded provisions for general user protection: Law No. 1/2024 regulate broader provisions against hate speech, online threats, and hoax. 	<p>Law No. 1/2024 offers increased protection for vulnerable groups like children and aims to create more secure and ethical online environment for the general users.</p> <p>With the specific responsibility of child protection under the Law No. 1/2024, ESPs are expected to adopt system upgrades and operational changes to adhere the obligation of child protection. The potential administrative sanctions of non-compliance further emphasized the urgency for ESPs to prioritize child protection measures.</p>
Electronic Transactions and Contracts	<ul style="list-style-type: none"> No specific protection for high-risk electronic transaction. No requirement to use Indonesian law as the governing law of international electronic transactions. 	<ul style="list-style-type: none"> High-risk electronic transactions to use Electronic Signature secured by Electronic Certificate. Standard clause on Electronic Contract must use Indonesian law as governing law if: (i) the user of the ESP’s platform is from Indonesia and provide its consent in Indonesia jurisdiction; (ii) performance of the contract is within the 	<p>Requirement to use e-signatures secured with e-certificate aims to strengthen the authentication and verification process in high-risk transactions. This may reduce the potential fraud and identity theft during such transactions. Consequently, ESPs are expected to be more accountable for ensuring their systems and processes meet</p>

		Indonesia jurisdiction; and/or (iii) ESP has a business place or undertake its business in Indonesia.	<p>stricter security standards in handling high-risk transactions.</p> <p>ESPs, particularly engaged in online services and digital goods, may need to adjust its standard contracts to comply with the requirement to utilize Indonesian law.</p> <p>While such requirement reinforced the legal certainty and predictability for Indonesian/foreign users and businesses, imposing Indonesian law by default might limit parties' ability to choose more suitable jurisdictions for more complex international transactions.</p>
Digital Criminal Offenses	<ul style="list-style-type: none"> Limited provision on content and behavior. Clause on digital defamation offense is generally regulated and provide no precise boundaries. 	<ul style="list-style-type: none"> Digital criminal offense expanded to include: <ul style="list-style-type: none"> (i) hate speech and discriminatory content¹; (ii) dissemination of false or misleading information (hoax) which cause public disruption²; (iii) coercing people with threats of violence or defamation or with the threat of revealing secrets³. Previous defamation offense clause revoked and newly formulated to provide clearer elements i.e. to 'attack someone's dignity or reputation by accusing them of something, with the intention of making it known to the public.' 	<p>The expanded category of criminal offenses provides clearer framework for ESP's in addressing harmful content and behavior on digital platforms. On individual level, these provisions deter and encourage users to use social media responsibly and avoid distribution of harmful online content.</p> <p>The pre-amendment clause lacked clear boundaries which practically led to misinterpretations and inconsistent application. The new clause specifically defines the elements of digital defamation which provides better guidance for both accused and prosecutors, potentially leading to fairer and more predictable outcomes.</p>
Protection Against False Accusation	No specific protection for the parties who wrongfully accused of criminal act of defamation through digital platform.	Making untrue and unproven accusations regarding defamation is criminally punishable.	Previously, individuals falsely accused of digital defamation lacked specific legal protection causing reputational damage.

¹ Article 28A paragraph (2) of Law No. 1/2024

² Article 28A paragraph (3) of Law No. 1/2024

³ Article 27B of Law No. 1/2024

			The amended law specifically criminalizes making untrue and unproven defamation accusations, creating the deterrence and accountability for online behavior.
Civil Servants Investigator Authority	No authority to order any related ESP to terminate access for the purpose of criminal investigation.	Civil Servants Investigator is now granted the authority to order any ESP to temporarily terminate access towards the social media account, bank account, electronic money, and/or digital asset of the accused.	The amended EIT Law grants Civil Servant Investigators increased access to digital accounts for criminal investigations, potentially improving efficiency and evidence gathering. However, further implementing guidelines/ regulation are critical to ensure the responsible and ethical use of this authority to protect individual rights in the digital landscape.

Criminal Provisions in Law No. 1/2024 and the New Criminal Code

While Law No. 1/2024 introduces new obligations for business actors, we view that its primary focus lies in amending or adding provisions related to criminal offenses committed through electronic systems. In light of the upcoming enforcement Law No. 1 of 2023 regarding Criminal Code (“**New Criminal Code**”) on 2 January 2026, criminal offenses clause under Law No. 1/2024 appears to align with the recently enacted New Criminal Code in several aspects.

Examples of this alignment can be seen in:

- Newly added Article 27B of Law No. 1/2024 regarding extortion, which mirrors the wording of Article 482 of the New Criminal Code.
- The similarity between Article 28 paragraph (3) of Law No. 1/2024 on hoax and Article 263 paragraph (1) of the New Criminal Code.

However, Law No. 1/2024 also introduces independent criminal offenses which not specifically covered under the New Criminal Code. These include:

- Article 28 paragraph (1): hoax causing loss to electronic consumers.
- Article 27A: defamation through electronic systems.

It is important to note that Article 622 paragraph (1) letter r of the New Criminal Code mandates the revocation of certain criminal offense clauses under the EIT Law upon its enforcement. However, the New Criminal Code remains silent on whether provisions enacted later under Law No. 1/2024 will be similarly revoked. This ambiguity leaves open the possibility that these offenses may remain applicable even after the New Criminal Code comes into effect, potentially creating a dualistic criminal law framework.

Such absence requires attention and clarification by the government to ensure legal certainty and consistency in future applications.

Key Takeaways

In view of the foregoing, some of the key takeaways which may be taken for consideration include:

- a. Business actors are expected to comply with the new standards mandated by the Law No. 1/2024 specifically in the aspect of: (i) for ECP, to establish an Indonesian legal entity and to be domiciled within Indonesia; (ii) for general ESP, to adopt system upgrades and operational changes to adhere the obligation of child protection by through age checks, user verification, and abuse reporting; (iii) for ESP in digital goods/service, to adjust its standard transaction to utilize Indonesian law as the governing law.
- b. Individual and business should be aware of the newly introduced or enhanced criminal offenses under Law No. 1/2024 including: (i) dissemination of hate speech and discriminatory content; (ii) distribution of false or misleading information (hoax) that causes public disruption; (iii) coercing people with threats of violence or defamation or revealing secrets; (iv) criminalization of making untrue and unsubstantiated accusations of defamation.

Individuals are expected to pay more attention to their online conduct while businesses may want to consider updating its user guidelines/code of conduct to protect themselves for any criminal associated risks.

- c. Law No. 1/2024 primarily amends electronic crime provisions which aligns with the New Criminal Code in several areas. While some EIT Law offenses will be automatically revoked when the New Criminal Code takes effect in 2026, the applicability of additional provisions under Law No. 1/2024 – which enacted after the New Criminal Code in 2023 - remains unclear while potentially might still apply. This requires further guidance from the government to ensure legal consistency and smooth implementation of the criminal law.
- d. Currently, 4 (four) implementing regulations of Law No. 1/2024 consists of 2 (two) new Government Regulations, amendment of Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions, and amendment of Ministry of Communication and Information Ministerial Regulation No.50 of 2020 on Private Electronic System Operators are being prepared by government and expected to be issued by October 2024.

Navigating through the obligation of EIT Law can be intricate, and seeking professional legal assistance is highly recommended to protect your interest effectively. As legal experts in IT law and data protection, we are ready to assist you for tailored legal guidance in the digital landscape.

For further information and/or queries related to this alert, please contact:

Stefanus Brian Audyanto

Partner

Deloitte Legal Indonesia

Email: saudyanto@deloittelegal-id.com

Tammy A. Wenas Kumontoy

Managing Associate

Deloitte Legal Indonesia

Email: tkumontoy@deloittelegal-id.com

Michael I.H. Pandjaitan

Senior Associate

Deloitte Legal Indonesia

Email: mhalomoan@deloittelegal-id.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Legal Indonesia is a Deloitte Legal practice in Indonesia. Deloitte Legal means the legal practices of DTTL member firms, their affiliates or their related entities that provide legal services. The exact nature of these relationships and provision of legal services differs by jurisdiction, to allow compliance with local laws and professional regulations. Each Deloitte Legal practice is legally separate and independent, and cannot obligate any other Deloitte Legal practice. Each Deloitte Legal practice is liable only for its own acts and omissions, and not those of other Deloitte Legal practices. For legal, regulatory and other reasons, not all member firms, their affiliates or their related entities provide legal services or are associated with Deloitte Legal practices

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2024 Deloitte Legal Indonesia