

**26 March 2020**

**To**

**Mr Johnny G. Plate**

Minister of Communications and Information Technology

Ministry of Communications and Information Technology (KOMINFO)

Jl. Medan Merdeka Barat no. 9,

Jakarta 10110 Indonesia

**Subject: AIC Submission on Regulation on Governance of Private Scope Electronic System Administrator**

Dear Minister Plate,

The Asia Internet Coalition (AIC) and its members express our sincere gratitude to the Ministry of Communications and Information Technology (KOMINFO) for the opportunity to submit comments on the **Regulation on Governance of Private Scope Electronic System Administrator (ESA) (“Regulation”)**.

The AIC is an industry association comprised of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our member companies would like to assure KOMINFO that they will continue to actively contribute to the security of digital platforms, products and services in support of the digital economy goals of Indonesia. Our members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, Grab, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media), and Booking.com.

While we commend KOMINFO’s efforts to develop a legal framework for electronic system administrators, we express our concerns on the requirements imposed under the Regulation and suggest that they be aligned with global best practices. We urge KOMINFO to consider the potential consequences of the Regulation in order to prevent any unintended consequences in the longer run.

As such, please find appended to this letter detailed comments and recommendations, which we would like KOMINFO to consider when drafting the **Regulation on Governance of Private Scope ESAs**. We are grateful to KOMINFO for upholding a transparent, multi-stakeholder approach in developing this regulation. Furthermore, we welcome the opportunity to offer our inputs and insights on industry best practices, directly through meetings and discussions and help shape the dialogue for the advancement of the digital ecosystem in Indonesia.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at [Secretariat@aicasia.org](mailto:Secretariat@aicasia.org) or +65 8739 1490. Thank you for your time and consideration.

Sincerely,



**Jeff Paine**  
**Managing Director**  
**Asia Internet Coalition (AIC)**

**Cc:**  
**Mr. Samuel A. Pangerapan**  
Director General of Informatics Application  
Ministry of Communication and Informatics

**Cc: Ms. Mariam Barata**  
Director of Informatics Application Governance  
Directorate General of Informatics Application  
Ministry of Communication and Informatics

## Detailed Comments on Regulation on Private Electronic System Operators

---

### 1. Definition of “Private Scope Electronic System Administrator” (Chapter 1, General Provisions, Article 1)

We are of the view that the definition of “Private Scope Electronic System Administrator” is not clear. Specifically, the definitions of “person” and “business entity” are not clear. “Private Scope Electronic System Administrator” means the administration of an Electronic System by a person, business entity, and the community. Therefore, clear definitions of “person” and “business entity” need to be provided in the Draft Regulation. Furthermore, the definition of “Foreign Private Scope Electronic System Administrator (ESA)” is not available in the existing Draft Regulation.

**Recommendation:** Article 1 shall be amended with the following definitions:

- “Person means Indonesian citizens and Business Entities”
- “Business Entity means a business entity established in Indonesia under Indonesian law”
- “Private Scope Electronic System Administrator means the administration of Electronic System by a Person, Business entity, and the community”
- “Foreign Private Scope Electronic System Administrator (ESA) means the administration of Electronic System by a foreign citizen or a foreign business entity”

### 2. Definition of “prohibited content” (Chapter 1, General Provisions)

The Draft Regulation does not provide a comprehensive explanation of what would constitute prohibited content - apart from expressly mentioning pornographic and gambling related content in several articles. The Draft Regulation merely provides how prohibited content is classified into three categories:

- (i) in violation of laws and regulations
- (ii) causing anxiety to the society and disturbing public order
- (iii) posting means or providing access to prohibited content

**Recommendation:** There should be a clearer way to identify the scope of the prohibited content. For instance, explicitly mention the higher regulation that the draft regulation is used as reference to determine prohibited contents.

### 3. Application to Cloud Service Providers (Articles 1 and 3)

As Cloud Service Providers (“CSPs”) do not control customer data – and in fact lack visibility to distinguish the nature of such content – many provisions in the regulation (e.g., Articles 13 and 16) are impractical for CSPs to implement and would make their business model unsustainable in Indonesia. These requirements are also contrary to international norms that third party service providers cannot be held liable for customer content about which they had no knowledge.

Furthermore, the penalties described in the regulation – e.g., termination of access to an Electronic System Administrator (ESA) by an Internet Service Provider (Articles 21-24) – would be grossly disproportionate as applied to a CSP because it could result in termination of access to the CSPs’ services for all customers in Indonesia (in contrast, terminating access only to the party that is directly responsible for publishing unlawful content has a more limited scope and appears to be consistent with the intent of the regulation, as reflected in the [Annex: Landing Page Design](#)). These penalties could also have unintended consequences by resulting in the loss of internet access to thousands of Indonesian businesses and the loss of thousands of Indonesian jobs.

**Recommendation:** It is therefore critical that the regulation make clear in Article 1 that references in the regulation to ESAs do not apply to CSPs except where the regulation explicitly refers to “Private Scope ESA that operates cloud computing services.” Article 3(1) should be amended as proposed above for the same reason.

### 4. Potential extra-territorial effect and registration of private scope ESA (Articles 1 and 5)

According to Article 5, foreign private scope ESA which meets the requirements as referred to in the Article 3 paragraph (1) and conducts businesses and/or activities in Indonesia shall be obligated to undertake the registration and reporting certificate of domicile and/or certificate of incorporation. The scope of *conducts businesses and/or activities in Indonesia* is not clear. More clarity should be provided on this matter. There should also be a certain threshold that needs to be met.

**Recommendation:** It would not be practicable or enforceable for Indonesia to exercise extra-territorial effect of Indonesian laws on foreign/offshore ESAs. In line with global laws on privacy or electronic transactions, we propose that the regulation should apply only to entities formed or recognized under the laws of Indonesia.

**Article 5 paragraph (1) shall read as follows:**

“Foreign Private Scope ESA which meets the requirements as referred to in the Article 3 paragraph (1) and conducts businesses and/or activities in Indonesia shall be obligated to undertake the registration. Conducting businesses and/or activities in Indonesia means (i) actively marketing the Foreign Private Scope ESA’s business to Indonesian citizens

in Indonesia and (ii) gaining revenue above the equivalent of USD100,000 from Indonesian citizens in Indonesia, for a consecutive 12-month period.”

## 5. Localization requirements (Chapter II, Article 6)

According to the regulation, all private ESAs, including foreign Private ESA that conduct business activities in Indonesia must register with KOMINFO as a Private ESA. Private ESAs that fail to register with KOMINFO will be subject to sanctions, ranging from administrative sanctions in the form of warning letter to blocking access to the Private ESA’s platform by KOMINFO.

According to the Article 6 the management, processing, and/or retention of Electronic System and Electronic Data outside of the territory of Indonesia, Private Scope ESA shall be obligated to have an approval from the Minister taking into account the requirements and consideration of national interests included in order to ensure the effectivity of the supervision and law enforcement.

The draft regulation does not further elaborate as to how to determine that a foreign private ESA is “conducting business activities in Indonesia” and therefore it can be perceived that all foreign private ESAs must be registered in Indonesia, regardless of scale, potential risks, or type of activities.

Additionally, as the registration of Private ESAs must be carried out via the OSS system, it is still unclear how foreign Private ESAs will be able to register themselves via the OSS system, since it currently can only be used for licensing of Indonesian entity.

This provision contradicts the data localisation provision set under the GR71 regulation which allows Private ESAs to store data offshore.

The draft regulation also does not specify the detailed requirements and criteria to obtain approval from KOMINFO in order to manage, process, and/or store electronic systems and data offshore. Therefore, until there is further specific regulation on this matter, it might be likely that the approval for maintaining data outside Indonesia will be at the sole discretion of KOMINFO.

**Recommendation:** We recommend elaborating more on the definition of and scope of ‘conducting business activities’, whether there are specific measures to determine this (e.g size, type of operations, etc). We also recommend changing the provision so that registration applies only for local companies, as it is done through OSS.

KOMINFO must not impose new restrictions on cross-border data transfers by pursuing mechanisms that force onshore data residency. Data localization requirements will have a significant impact on existing Indonesian businesses who have come to rely on the low cost, robust security and easily scalable benefits of offshore cloud services.

Government of Indonesia must honor its commitment in GR71 to allow “Private” ESAs to store their data outside of Indonesia, and to provide a two-year transition period for “Public” ESAs to comply with processing and storing their data onshore. This provision is inconsistent with GR71 that does not require any prior approvals for Private ESAs to store and process data outside the territory of Indonesia. Article 6, therefore, should be deleted, as it could potentially be a setback to the progressive regulatory approach that was taken by the government previously.

Countries that enact barriers to data flows make it harder and more expensive for their businesses to gain exposure and to benefit from the ideas, research, technologies, and best practices that accompany data flows and the innovative goods and services that rely on data. Restrictions on cross-border data flows also create trade barriers and impact business models. Studies show that data localization and other barriers to data flows impose significant costs: reducing U.S. GDP by 0.1-0.36%; causing prices for some cloud services in Brazil and the European Union to increase 10.5 to 54%; and reducing GDP by 0.7 to 1.7% in Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam, which have all either proposed or enacted data localization policies.

On the contrary, cross-border data flows can enhance data security in technologies such as cloud computing by allowing greater geographic diversity for data storage. Cross-border data flows are essential to trade and for companies to make the most of the global economic opportunity. International flow of data contributed USD2.8 trillion to the global economy in 2014, a figure that could reach USD11 trillion by 2025. Over the past decade, data flows have increased world GDP by 10.1%. Thus, enabling cross-border data flows could result in a positive impact on Indonesia’s GDP and support the government’s objective of producing more tech unicorns and even a hectocorn — a start-up valued at \$100 billion.<sup>1</sup>

This is supported by the evidence that efforts to reduce barriers to cross- border data traffic have been shown to drive growth.

## **6. Registration of private scope ESA (Chapter II, Article 8, Para 4 and 5)**

**Article 8 paragraph (4):** Private Scope ESA shall be obligated to fulfill the registration information which have not been fulfilled in 7 (seven) business days as of the receipt of the notification letter to fulfill the registration requirements as referred to in the paragraph (2).

**Article 8 paragraph (5):** In the context of Private Scope ESA which does not fulfill the registration requirements in 7 (seven) business days as referred to in the paragraph (4), The Minister shall give a refusal on the registration of the Private Scope ESA.

The period provided (7 business days) to fulfil the requirement is too short.

<sup>1</sup> <https://en.tempo.co/read/1263684/kominfo-to-boost-unicorn-startups-eyes-the-birth-of-hectocorn>

**Recommendation:** We recommend replacing 7 (seven) days to 30 (thirty) business days. *Article 8 paragraph (4) shall read as follows:* “Private Scope ESA and Foreign Private Scope ESA shall be obligated to fulfill the registration information which have not been fulfilled in 30 (thirty) business days as of the receipt of the notification letter to fulfill the registration requirements as referred to in the paragraph (2).”

*Article 8 paragraph (5) shall read as follows:* “In the context of Private Scope ESA and Foreign Private Scope ESA which does not fulfill the registration requirements in 30 (thirty) business days as referred to in the paragraph (4), the Minister shall give a refusal on the registration of the Private Scope ESA.”

## 7. Unblocking of the platform following a termination of access/blocking (Chapter II, Article 12)

Normalization in this context means the unblocking of the platform following a termination of access/blocking. Article 12 does not contain normalization for Foreign Private Scope ESA that never tried to register itself with the Minister. Article 12 should also contain normalization for Foreign Private Scope ESA that never tried to register and then be subjected to termination of access by the Minister as indicated under Article 11 paragraph (2).

*Article 12:* “The Minister shall be conducting the normalization on the termination of access as referred to in the Article 11 paragraph (3) after the Private Scope ESA fulfills the registration provisions as referred to in the Chapter II.”

**Recommendation:** To include Article 11 paragraph (2) in this context so that the entire Article 12 shall read as follows:

“The Minister shall be conducting the normalization on the termination of access as referred to in the Article 11 paragraph (3) and Article 11 paragraph (2) after the Private Scope ESA fulfills the registration provisions as referred to in the Chapter II.”

## 8. Illegal content takedown (Articles 16.1, 16.3, 21.8, 22.8 )

8.1. **Articles 16.1 and 16.3** implicitly require user-generated-content platforms to perform pre-emptive content moderation and interception, which is burdening the platforms in two areas: (1) changes of global policy, rules and terms of services; (2) investment in human resources and technology for pre-emptive detection of the illegal content. While the second is more practically feasible than the first one, it still needs a lot of time and resource investment before it is put in place. In addition, Article 16.3b only gives the platform a total of 12 hours to comply with the administrative fine that can be applied without notice.

The 1x24 hours period is too short to conduct an assessment and to terminate access over prohibited Electronic Information/Electronic Document containing gambling and pornographic contents.

Article 16 paragraph (3) is unclear as to when the period for Private Scope ESA to take down the content begins, considering absence of a warning letter from the Minister. This seems to be on a self-assessment basis and therefore needs to be clearly stated that such prohibited content will be taken down within 7x24 hours as of the date of the existence of such prohibited content is recognized by the Private Scope ESA.

We are concerned that provisions in Article 16 will have negative implications for freedom of speech in Indonesia.

- First, the scope of the content which falls under these provisions is not clearly defined, in particular as to what constitutes content which disturbs the public order. In order for platforms to have legal certainty as to what this entails, and to ensure that the law is used in a manner which is consistent with freedom of expression, these restrictions should be clearly defined.
- Second, the proactive removal of pornography and gambling is problematic, given that it is technically impossible for global platforms to identify content which violates specific national laws for removal.
- Third, these restrictions would prejudice smaller platforms to an even larger degree than established market players. The operational needs to meet these requirements are enormous, and it would not be practical or feasible to expect industry players - particularly smaller ones who are resource constrained - to comply with them.

**Recommendation:** There should be at least a grace period in place for the platform to make changes to comply with the regulation. The AIC recommends following the grace period provided by GR71/2019.

Moreover, the administrative fine in place should be with notice. Or else, the platform might fall into the condition where they have to face termination of access, before realizing that there are administration fines in place.

We recommend amending Article 16 paragraph (3) to be read as follows:

“In the context of Private Scope ESA, whose provision , broadcast, upload, and/or exchange of their Electronic Information and/or Electronic Document conducted by the Electronic System User (User Generated Content), which does not conduct termination the access over the Prohibited EI/ED as referred to in the paragraph (1) in the period of 7 x 24 (seven times twenty four) hours since the date of such Prohibited EI/ED with the gambling content is recognized by the Private Scope ESA shall be imposed with administrative sanctions in a form of:

- a. a direct administrative sanction without prior warning with periodic increase every 1 x 4 (one times four) hours, maximum administrative sanctions of 3 (three) times of periodic increase;

- b. the termination of access after the imposition of fine as referred to in the point a is reached.”

There should be an approved process through which one authorised regulator (i.e. KOMINFO) is able to send takedown requests to platforms. Platforms should be obliged to:

- a. have a reporting channel to receive these TDRs, review them, and take action as appropriate.
- b. prioritise content which may lead to imminent harm to lives or which may cause injury. Such content should be removed as expeditiously as possible.
- c. review and take action on all other categories of content in a timely way. Platforms should be permitted sufficient time to review such content.

## 8.2. Article 21. 6

The 2x24 hours period is too short for the Private Scope ESA to terminate access to prohibited Electronic Information/Electronic Document contents, after receiving an order from the Minister to terminate access.

**Recommendation:** We suggest replacing the stipulated period with 7x24 hours period.

8.3. Article 21. 8 and 22.8 requires a platform to remove “illegal content with urgent nature” within two hours after a request is filed by the Ministry. However, there is no clear definition on what constitutes causing anxiety to the society and disturbing public order (*konten yang meresahkan masyarakat dan mengganggu ketertiban umum*) as stipulated in Article 20.2. This is open to multiple interpretations of the situation and therefore susceptible of being misused on political grounds. Also, taking into account that platform management is in a different time zone that could affect time of response from the platform.

The 2 hours period is too short for the Private Scope ESA to terminate access to prohibited Electronic Information/Electronic Document contents containing terrorism acts and causing public unrest and disturbing public order, after receiving an order from the Minister or authorized ministry or institution to terminate access based on the request from the public.

A turnaround time of 2 hours is not operationally feasible. Platforms such as Facebook are already prioritising removing content which may cause imminent harm. There are also unintended and perverse consequences of resourcing to prioritize these escalations instead of addressing potentially more consequential harmful content. On top of it, imposing a strict 2 hour TAT would require platforms to break with international norms and best practices, and to remove content without any form of review to avoid incurring legal liability. This would lead to an extremely high risk of over-enforcement.

**Recommendation:** The draft regulations should have clearer definitions and indicators/parameters on what constitutes “causing anxiety to the society and disturbing public order”. The AIC recommends changing the response time limit put in place in the draft regulations to 24 hours for illegal content with urgent nature, and 3-5 working days for non-urgent illegal content.

## 9. Specific responsibilities of Private ESAs (including CSPs) on Law Enforcement (Articles 17, 18, 29, 30)

According to the draft regulation, Private ESAs are required to provide access to their electronic systems and/or data to (i) ministries or government institutions for monitoring purposes, and (ii) law enforcement for law enforcement purposes. The access must be granted within 24 hours after receiving the request.

It is as yet unclear whether this request will apply to offshore entities merely for monitoring purposes.

A few separate issues to note are:

- a. We will need clarification on the terms ‘providing direct access to systems and data’ as this is uncommon to be done.
- b. There is also a lack of the type and criteria of data that should be disclosed, as it may range to every type of data from Personally Identifiable Information (PII) to internal company data.
- c. There is no differentiation in terms of turnaround time, where it should actually distinguish between emergency and non-emergency situations.

In a cloud computing environment, CSPs typically do not have visibility of their customers’ data, and hence will not be able to establish the purposes of that processing or proactively monitor unlawful content. Therefore, CSPs cannot reasonably be expected to monitor, or required to access, data processed using their services. Indeed, they often technically cannot do so. Requests to remove unlawful content should therefore be directed to the persons responsible for publishing that content, not CSPs.

**Recommendation:** We strongly recommend that the provisions related to ‘access’ to the systems of Private ESAs or a fixed Turnaround time be removed. We therefore would propose high level principles of cooperation. Any requirements on access to Personal Data must be aligned with the principles of Personal Data Protection (PDP) which have been included in the draft PDP bill submitted to the parliament.

The AIC urges KOMINFO to work with Private ESAs including digital platforms and CSPs to ensure that any applicable ESA requirements on data, monitoring and law enforcement access are consistent with the above principles and allow CSPs and ESAs generally to respond in meaningful and productive ways to legitimate law enforcement requests.

## 10. Content takedown request mechanism

The draft regulation only explicitly mentioned electronic mail as the means of communication between Government/Law Enforcement and the platform. Most of the global digital platforms, including AIC member companies, already have online form mechanisms in place specifically for the government/Law enforcement to use.

**Recommendation:** The draft regulation should explicitly recognize the online mechanisms already provided by platforms by adding a sentence “*Jika tidak ada mekanisme khusus lain yang disediakan oleh PSE*” (translation: If there is no other specific mechanism provided by the platform) after the phrase “surat elektronik” in all related articles.

### Annex: Landing Page Design

