COMMENTS ON DRAFT REGULATION OF THE MINISTER OF COMMUNICATIONS AND INFORMATICS CONCERNING PUBLIC SCOPE ELECTRONIC SYSTEM OPERATORS

October 16, 2023

On behalf of BSA | The Software Alliance (**BSA**)[1] and the Global Data Alliance (**GDA**),[2] we thank the Ministry of Communication and Informatics (**KOMINFO**) for soliciting feedback from the private sector on the Draft Regulation of the Minister of Communications and Informatics Concerning Public Scope Electronic System Operators (**Draft Regulation on Public ESOs**).[3]

I. Introduction

We recently provided comments to KOMINFO on the Draft Implementing Regulation of Law Number 27 of 2022 Regarding Personal Data Protection (**Draft PDP Regulation**) (BSA comments[4])(GDA comments[5]). BSA provided comments on a joint industry association letter on the Public Electronic Service Providers Draft Regulation.[6] BSA also commented in past joint submissions on the Draft Personal Data Protection Bill in 2019[7] and the Draft Amendment of Government Regulation 82/2012 on Electronic Systems and Transaction Operations in 2018.[8]

We offer two main recommendations in this submission:

1. Amend Article 95(1) to allow Public ESOs to use either cloud computing services provided by the National Data Center or third-party Cloud Computing services as long as they meet the requirements of Article 96.

2. Extend the comment deadline by one month to allow for more detailed and meaningful public sector input until November 16, 2023.

---

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Palo Alto Networks, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] GDA members are headquartered across the globe and are active in many different sectors. See www.globaldataalliance.org.

[3] See https://www.kominfo.go.id/content/detail/51992/siaran-pers-no-351hmkominfo102023-tentang-konsultasi-publik-rpm-penyelenggara-sistem-elektronik-lingkup-publik/0/siaran_pers

[4] See https://www.bsa.org/policy-filings/indonesia-bsa-comments-on-draft-implementing-regulation-of-law-number-27-of-2022-regarding-personal-data-protection

[5] Global Data Alliance, Comments on Draft Implementing Regulation of Law Number 27 of 2022 Regarding Personal Data Protection (Sept. 25, 2023), https://globaldataalliance.org/wp-content/uploads/2023/09/09252023gdabhasadatapro.pdf

[6] See https://www.bsa.org/policy-filings/indonesia-joint-association-input-letter-on-public-electronic-service-providers-draft-regulation

[7] See https://www.bsa.org/policy-filings/indonesia-usabc-bsa-comments-on-draft-indonesia-personal-data-protection-bill

[8] See https://www.bsa.org/policy-filings/indonesia-bsa-joint-submission-on-gr82-amendment-matrix

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

II. About BSA and GDA

BSA is the leading advocate for the global software industry. Our members are enterprise software companies that create business-to-business technologies that help organizations of all sizes and kinds to innovate and grow. For example, BSA members develop and provide tools including cloud storage and data processing services, customer relationship management software, human resource management programs, identity management services, and collaboration software. BSA offers our extensive global experience in technology policy to serve as a resource and we hope that our comments in this submission will be helpful to KOMINFO.

The GDA is a cross-industry coalition of companies that are active in many sectors of the economy and headquartered around the world. GDA member companies are committed to high standards of data privacy, data security, and data responsibility which relies on the ability to transfer data in real time across digital networks to innovate and create jobs. The GDA supports policies that help instill trust in the digital economy while safeguarding the ability to access technology and share knowledge and information data across borders.

BSA and GDA members share a deep and long-standing commitment to protecting data across technologies and business models as they recognize that today's cross-border economy depends on the trust of customers and the public.

III. General Comments

As reflected in the GDA's Cross-Border Data Policy Index,[9] the ability to access technology and transfer data securely across international digital networks is of central importance to both economic and other governmental policy objectives: Not only do restrictive cross-border policies fail to protect privacy;[10] they also hurt developing countries[11] and small businesses;[12] impede financial inclusion;[13] undermine cybersecurity;[14] slow innovation;[15] and impair various health and safety,[16] environmental,[17] and other regulatory compliance goals (including anti-corruption, anti-money laundering, fraud prevention, etc.).[18] Data transfers are critical to economies across all sectors[19] at every stage of the value chain.[20] The United Nations, World Trade Organization, World Bank, and other development banks have warned that data localization mandates and data transfer restrictions are particularly harmful to developing economies.

[9] https://globaldataalliance.org/resource/cross-border-data-policy-index/

[10] https://globaldataalliance.org/issues/privacy/

[11] https://globaldataalliance.org/issues/economic-development/

[12] https://globaldataalliance.org/issues/small-businesses/

[13] https://globaldataalliance.org/sectors/finance/

[14] https://globaldataalliance.org/issues/cybersecurity/

[15] https://globaldataalliance.org/issues/innovation/

[16] https://globaldataalliance.org/sectors/biopharmaceutical-rd/; https://globaldataalliance.org/sectors/medical-technology/; https://globaldataalliance.org/sectors/healthcare/

[17] https://globaldataalliance.org/issues/environmental-sustainability/

[18] https://globaldataalliance.org/issues/regulatory-compliance/

[19] https://globaldataalliance.org/wp-content/uploads/2021/07/GDAeverysector.pdf

[20] https://globaldataalliance.org/wp-content/uploads/2021/07/infographicgda.pdf

IV. Recommendation: Remove *De Facto* Data Localization from Articles 94-95

Article 93 provides for Public ESOs to utilize cloud computing services by the National Data Center and/or third parties. Article 94(1) requires Agencies to use Cloud Computing Services provided by the National Data Center. However, Article 95(1) states that "[i]n the event that the availability of Cloud Computing services provided by the National Data Center cannot meet the capacity needs of the Public ESO, the Public ESO can use third-party Cloud Computing services as intended in Article 93(2)(b)." This essentially requires Public ESOs to locate their data within the National Data Center, which is a form of de facto data localization.

To enhance data safety and security, we urge a flexible approach allowing Public ESOs and government agencies to choose cloud providers based on their specific security needs. Reliance solely on the National Data Center can lead to a false sense of security, is not a guarantee against security breaches, and may create a single point of failure.[21] Furthermore, to foster market access and innovation, we encourage an open attitude toward international cloud providers, provided they adhere to relevant data security standards. To promote a thriving digital economy, the emphasis should be on cultivating collaboration between government agencies, private cloud providers, and international technology firms, stimulating innovation and economic growth while avoiding overly protectionist policies that could hinder access to global technology resources.

Impact on Cybersecurity of Public ESOs

The requirement in Article 95(1) will restrict Public ESOs from using world leading information technology (**IT**) and cloud computing solutions from service providers that offer their services from outside of the National Data Center. Such services frequently provide best in class security capabilities, and restricting Public ESOs from using such services may expose them to greater data security risks. Additionally, Public ESOs may want to store data in geographically diverse locations to obscure the location of data to reduce risks of physical attacks, to reduce network latency, and to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location, whether such damage might be caused by natural causes, accidents, or intentional acts.

Impact on National Security in Indonesia

Overbroad data localization mandates tend to undermine — rather than enhance — national security for many of the cybersecurity reasons noted above. One model for protecting national security in the procurement of ICT and cloud services, which we commend to Indonesia's attention, can be found in the US Federal Risk and Authorization Management Program (**FedRAMP**). This program promotes the adoption of secure cloud services across the US government by providing government agencies a consistent approach to security and risk assessments of cloud services. In the context of government information stored in the cloud, sensitive data is typically more secure when it is protected via a distributed cloud architecture bolstered by the strongest possible security protocols. For example, the decision of Ukraine to adopt such a distributed and strengthened security posture protected it from cyberattacks directed at Ukraine, before and after the February 2022 invasion.

Specific Recommendation

In light of the foregoing considerations, we **propose amending Article 95(1) to allow Public ESOs to use either cloud computing services provided by the National Data Center or third-party Cloud Computing services as long as they meet the requirements of Article 96**.

[21] *See generally,* Global Data Alliance, Cross-Border Data & Cybersecurity (2023), at: https://globaldataalliance.org/issues/cybersecurity/ (explaining that restrictions on cross-border access to, or movement of, security data may harm the ability to share research, identify threats, and develop mitigations to protect governments, businesses, and individuals around the world from attack. Mandates to localize security data can harm incident response, the ability for organizations to manage cybersecurity in an integrated way, and the security data analytics to counter malicious cyber activity.)

Specifically, we recommend (1) amending Article 94(1) to allow Agencies to use Cloud Computing Services provided by third parties in addition to the National Data Center, and (2) deleting the first part of Article 95(1) as follows: "~~[i]n the event that the availability of Cloud Computing services provided by the National Data Center cannot meet the capacity needs of the Public ESO,~~ the Public ESO can use third-party Cloud Computing services as intended in Article 93(2)(b)."

V. Recommendation: Allow sufficient time for engagement with private sector

We appreciate the opportunity to take part in the public consultation. We respectfully urge enhancing the engagement process by extending the timeframe for public input on measures of these kinds. Industry and other stakeholders were only provided two weeks from publication to translate and review the Draft Regulation on Public ESOs, consult with our member companies, and develop our recommendations. Two weeks is simply not enough time to provide thoughtful input on any policy, let alone one as extensive as the Draft Regulation on Public ESOs. Allowing a longer timeframe to review and respond to the extensive Draft Regulation on Public ESOs would enable industry stakeholders to provide more detailed and thoroughly considered recommendations.

Specific Recommendation

As discussed in our recent comments on the Draft PDP Regulation, providing adequate time and opportunity for industry engagement on draft rulemaking will better assist KOMINFO to achieve its regulatory goals. We kindly request KOMINFO to extend the deadline for comments by one month beyond October 16, 2023 and provide further opportunities for industry engagement as you finalize these rules.

VI. Conclusion

We appreciate the opportunity to provide our comments and recommendations on the Draft Regulation on Public ESOs. We hope that our comments will assist in the development of regulations that allow Public ESOs to maintain cybersecurity and promote innovation. We urge KOMINFO to continue engaging with the private sector on how to further improve the Draft Regulation on Public ESOs. Please do not hesitate to contact the undersigned at waisanw@bsa.org to continue the discussion.

Yours faithfully,

Wong Wai San

Wong Wai San

Senior Manager, Policy – APAC