March 1, 2018

H.E. Rudiantara
Minister
Ministry of Communication and Information Technology
Jalan Medan Merdeka Barat No. 9
Jakarta 10110, Republic of Indonesia

Dear Minister Rudiantara,

The American Chamber of Commerce Indonesia, American Council of Life Insurers, BSA | The Software Alliance, the Information Technology Industry Council, the US-ASEAN Business Council, and the U.S. Chamber of Commerce express our gratitude to the Ministry of Communication and Information Technology of Indonesia ("KOMINFO") for the opportunity to share our comments on Government Regulation 82/2012 on Electronic Systems and Transaction Operations ("GR82") and the draft amendment shared with us by the Minister on February 1, 2018 ("Draft Amendment").

We understand the hard work that has been done by the joint Government of Indonesia teams to revise GR82. We are pleased that the Draft Amendment amends GR82 to allow "high electronic data" and "low electronic data" to be stored and processed outside Indonesia. Mandating data localization can reduce opportunities for Indonesia, lower service levels, create cyber security risks and raise costs, and we support the Government of Indonesia for narrowing this requirement to only "strategic electronic data." However, we remain concerned about certain provisions that remain unclear or are potentially problematic in the implementation.

In particular, we are concerned about 3 aspects of the Draft Amendment that appear to extend the nature of strategic services or public services to matters beyond national security, law and order, and the public interest. These are:

1. **The wide scope of what is an "electronic systems operator for public services";**
2. **The wide definition of "strategic electronic data"; and**
3. **Certain consequences of being deemed as an "electronic systems operator for public services."**

Our concerns under headings 1 & 2 above reflect the impracticability of the wide scope of the concepts of "strategic electronic data" and "electronic system operators for public services" and other related concerns. The wide scope of these two terms results in practically every website and electronic system (and their operators) being subject to the domestic processing and storage requirements, and goes beyond the intent of the proposed revisions to capture only those activities which are of a strategic nature.

We recommend that this scope be significantly narrowed down to include only electronic system operators whose activities directly relate to matters of national security, law and order, and public interest. It should also be consistent with the definition of public services under the existing public services law of Indonesia. In this respect, we would like to request that the definition of "strategic electronic data" exclude demographic data and Indonesia citizen data. In the explanatory notes to the

Draft Amendment, it was already implied, through examples, that such secondary data processed by the businesses would be considered only high and low electronic data. This is to avoid the situation where sectoral regulators would come back to KOMINFO with the inclusion of this secondary data processed by the businesses in the definition of "strategic electronic data", which we believe is not the intention of the Draft Amendment.

Our concerns on heading 3 above relate to the risks of data localization There are certain consequences of being deemed as an "electronic systems operator for public services," particularly strategic electronic data being subject to localization requirements. The collation of such important data in one geographical location by all electronic system operators across multiple industries only creates security risks as it creates an attractive target for cyber-criminals to focus their attacks on. It also concentrates the risk for important services relying on such data into these few points of failure, which would be ill-advised from an overall risk management perspective. Further, if data is restricted to remain in only one country, multiple data centers would be required in the same country and increased costs would likely be passed along to the consumer.

Spreading data across multiple jurisdictions provides much better resiliency and redundancy than local storage in the face of disasters. In a cloud environment specifically, companies may link multiple data centers, with data and applications replicated so that if one data center goes offline, the work can shift to another data center. This requires the ability to move data, often across borders (in compliance with applicable laws and regulations). The objective of ensuring access by local law enforcement to the data can be resolved, without introducing additional security risks, by ensuring that electronic system operators take appropriate security measures to protect such data.

Finally, we would like to highlight that across the world, electronic system operators are generally accepted to have different roles and characteristics that can be categorized into to two different functions with accompanying responsibilities: **data controllers** and **data processors/ intermediaries**, depending on how much control they have over the data in question. The differences between data controllers and data processors/intermediaries have been recognized by the OCED in their Privacy Guidelines[1] and by numerous jurisdictions worldwide, including Europe (in the European Union's General Data Protection Regulation), Singapore (in its Personal Data Protection Act 2012), and the Philippines (in its Data Privacy Act 2012). We strongly recommend that KOMINFO similarly distinguish between data controllers and data processors/intermediaries in GR82, by amending GR82 such that its obligations apply primarily to electronic system operators who are **data controllers**.

We respectfully submit the attached matrix, which explains our concerns in greater detail, seeks clarification on several provisions, and offers further recommendations for refining the Draft Amendment.

Electronic systems and online transactions present great opportunities for economic growth and improving the quality of life in Indonesia. Thus, it is important that policies that address these systems and transactions allow for flexibility and innovation so that the full potential of the digital sector can be realized. Our respective members are global leaders in ICT and have experience and expertise on how to manage electronic systems and data effectively and safely.

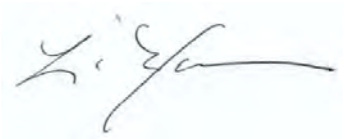
Our organizations and our respective members stand ready to work with the Government of Indonesia to further improve GR82 and the regime for regulating electronic systems in Indonesia. We

[1] Available at http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

are grateful to KOMINFO and the government inter-agency team for opening up the classification of high and low electronic data. We hope that our input will be useful to improve the current draft to avoid cumbersome potential problems in implementation. We also hope that this input will not delay the GR 82 Amendment further, as many industries regulated by the line ministries are waiting for this amendment to pass soon. We would welcome a meeting with KOMINFO to further discuss our concerns.

We thank you for considering our views

Sincerely,



Lin Neumann
Managing Director
AmCham Indonesia

Brad Smith
Chief International Officer
American Council of Life Insurers

Darryn Lim
Director, Policy - APAC
BSA I The Software Alliance

Josh Kallmer
Senior Vice President, Global Policy
Information Technology Industry Council

Alexander C. Feldman
President & CEO
US-ASEAN Business Council

Charles W. Freeman III
Senior Vice President, Asia
U.S. Chamber of Commerce

cc: The Hon. Joseph R. Donovan, Jr., United States Ambassador to Indonesia
H.E. Budi Bowoleksono, Ambassador of Indonesia to the United States

About the American Chamber of Commerce Indonesia
Formed in 1977, the American Chamber of Commerce (AmCham) Indonesia is a voluntary organization of professionals representing American companies operating in Indonesia. AmCham Indonesia promotes the business interests of its members by identifying and focusing on critical issues that improve the business climate, actively engaging stakeholders to achieve mutual understanding, serving as a key resource for business information and delivering forums for US business networks. Since its inception, AmCham has grown to more than 550 members and represents over 250 companies.

About the American Council of Life Insurers
The American Council of Life Insurers (ACLI) is a Washington, D.C.-based trade association with approximately 290 member companies operating in the United States and abroad. ACLI advocates in state, federal, and international forums for public policy that supports the industry marketplace and the policyholders that rely on life insurers' products for financial and retirement security. ACLI members offer life insurance, annuities, retirement plans, long-term care and disability income insurance, and reinsurance, representing 95 percent of industry assets, 93 percent of life insurance premiums, and 98 percent of annuity considerations in the United States. Learn more at www.acli.com.

About BSA | The Software Alliance
BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

About the Information Technology Industry Council
The Information Technology Industry Council (ITI) is the global voice of the tech sector and the premier advocacy and policy organization for the world's leading innovation companies. We advocate for global policies that advance industry leadership, open access to new and emerging markets, promote e-commerce expansion, drive sustainability and efficiency, protect consumer choice, and enhance worldwide competitiveness of our member companies.

About the US-ASEAN Business Council
For over 30 years, the US-ASEAN Business Council has been the premier advocacy organization for US corporations operating within the dynamic Association of Southeast Asian Nations (ASEAN). Worldwide, the Council's 150+ membership generates over $6 trillion in revenue and employ more than 13 million people. Members include the largest US companies conducting business in ASEAN, and range from newcomers to the region to companies that have been working in Southeast Asia for over 100 years. The Council has offices in: Washington, DC; New York, NY; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore.

About the U.S. Chamber of Commerce
The U.S. Chamber of Commerce represents the interests of more than three million U.S. businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations. Its International Affairs Division includes more than 50 regional and policy experts and 23 country-specific business councils and initiatives. It also works closely with 116 American Chambers of Commerce abroad.

MATRIX OF CONSOLIDATED DETAILED INPUTS/ COMMENTS ON DRAFT AMENDMENT TO GR82

Article No. and Content	Suggested Input/Recommendation	Comment
Article 1(4) – *'Electronic System Operator is any person, state agency, business entity, and community that provide, manage and/or operate Electronic System individually o jointly to Electronic System User for its interest or other party's interest'*	We recommend this minor revision in the language: "Electronic System Operator is any person, state agency, business entity, and community that provide, manage and/or operate Electronic System individually or jointly to Electronic System User for its interest or other party's interest, **with regards to each Electronic System Operator's function as data controller or data processor.** We also suggest including the following definitions of "data controller" and "data processor": "**Data controller is a party who is competent to decide about the contents and use of data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf.**" "**Data processor is a party who processes personal data on behalf of a data controller.**"	This aligns with our recommendation in the cover letter that KOMINFO distinguish between data controllers and data processors/intermediaries in GR82.
Article 3 – *'(1) Electronic System shall be operated by an Electronic System Operator.* *(2) Electronic System Operation as referred to in paragraph (1) shall be performed for:* *a. Public services; and* *b. Non-public services;*	We suggest adding the following paragraphs: "**(4) Electronic System Operator as intended in Paragraph (1) should have a function as data controller.**"	This is to apply the stricter requirements of GR82 to those who truly have control over the data in question (i.e., data controllers and not data processors).

(3) Criteria of public services as referred to in paragraph (2) shall refer to laws and regulations.'		
Article 5 – *'(1) Electronic System Operators for public services shall make obligatory registration.* *(1a) Electronic Systems Operator for public services that are required to register as stated in paragraph (1) includes:* *(a) Electronic System Operators that are regulated or supervised by Sectoral Supervisory and Regulatory Institution based on the provisions in the legislation.* *(b) State Operating Institutions of Electronic System Operator* *(c) Electronic System Operators that have:* *(1) Online portals, sites, or applications through internet that are used to facilitate offers and/or commercial goods and/or service;* *(2) Electronic systems that include online payment and/or financial transaction facilities through data communication network or internet.* *(3) Electronic systems that are used for electronic information processing containing or requiring fund deposit*	We recommend narrowing the definition of "Electronic System Operator for public services" as follows: • Omit Article 5(1a)(a) that states "*Electronic System Operators that are regulated or supervised by Sectoral Supervisory and Regulatory Institution based on the provisions in the legislation*". • Limit the services under Article 5(1a)(c) to: ○ government services; ○ services which are provided by private organizations to the government; and ○ specific services which are provided by private organizations which are identified to be strategic by sectoral regulators. We further recommend that: • The registration process should recognize the speed of digital developments and that the services being provided by electronic system operators will be continuously evolving to better serve the public; • The Ministerial Regulation should be issued in timely fashion manner; and • The registration should be granted as a matter of course where the electronic system operator in question meets the requirements for registration; and that the procedure should not include any discretion to withhold registrations.	In relation to **Article 5(1a)(a)**, we are troubled that an "Electronic System Operator for public services" would include "Electronic System Operators that are regulated or supervised by Sectoral Supervisory and Regulatory Institution based on the provisions in the legislation". This means that any company that is supervised or regulated by a sectoral regulator (e.g., OJK) would be considered an "Electronic System Operator for public services". Additionally, **Articles 5(1a)(c)(1) through 5(1a)(c)(6)** are currently so broad that they cover potentially any electronic system used to provide services to the general public (and their operators), no matter whether the system is actually public-facing; no matter how large or small the system is; and no matter how important the system is to national security, law and order, or the public interest. The regulation is contradictory to the existing Public Services Law and is likely to be unenforceable based on Indonesian law. It also restricts internet businesses that fuel innovation and the digital economy in the country. **Article 5(1a)(c)(4)** essentially states that any person that operates an electronic system that processes personal data and that serves the public, is an electronic system operator that provides a public service. This would mean that any website or system would be an Electronic System Operator that provides public service (no matter whether the system is public-facing or otherwise; no matter how large or small the system is; and no matter how important the system is to national security, defense or the public interest). For example, this wide definition would include foreign airlines, hotels, car rental companies, online travel and concierge services, real estate websites which lease foreign properties to Indonesian citizens. These

or items that are similar to fund deposit; *(4) Electronic systems that are used for processing, managing, or keeping data, including personal data for operational activities that provide services related to electronic transaction activities serve for the public; and/or* *(5) Electronic systems that are used for paid digital material transmission through data network, both by downloading through a portal/site, transmission through email or other applications to user's device.* *(6) Electronic systems that provide, manage, and/or operate communication services in the form of short message, voice call, video call, electronic mail, and online conversation (chatting/instant messaging), search engine, networking and social media, and digital provider services that may take the form of writing, voice, picture, animation, music, video, game, or combination of some and/all of them, including those provided through streaming or download.'*		websites collect personal data such as name, email address and payment details. It cannot be the intention that every single website that offers a good or service and collects Indonesian citizens' personal data must be processed within Indonesia and that the personal data is prohibited from leaving Indonesia. Having such a wide scope would be practically impossible given that the data must leave Indonesia in order for Indonesian citizens to book, rent or purchase a flight, hotel, car, tour or property before they travel overseas, or to purchase goods and services from foreign merchants. It is also necessary for data to be sent overseas for other practical and important reasons. For example, in order to identify and prevent fraud on electronic systems, it is necessary for data to be collected from across the world. Patterns of fraudulent activity which are collected from all over the world and analyzed in a centralized location help to improve fraud-prevention technology, which ultimately benefits Indonesian citizens. If Indonesian data is prevented from leaving Indonesia for fraud analytics, and such patterns of fraudulent activity cannot be identified in centralized platforms, and this would only benefit fraudsters and cyber-criminals. In this day and age where governments and organizations need to work together in the fight against fraud and cyber-criminals, the requirements in Article 5(1)(c) will unfortunately benefit criminals by reducing the effectiveness of fraud-prevention and cybersecurity tools. Another very routine and fundamental example where personal information may be transferred overseas includes transfers of employee personal information by multinational enterprises for human resource management purposes. Restricting such transfers would seriously impede the ability of foreign MNCs to effectively manage its workforce and provide benefits to Indonesia-based employees, thereby curtailing

		additional investments into the Indonesian domestic economy. **To narrow down the unduly broad definition of "Electronic System Operator for public services", we have thus recommended in the middle column of this table that Article 5(1a)(a) be omitted in its entirety, and that Article 5(1a)(c) either be removed from the Draft Amendment, or be redrafted to apply to only operators of electronic systems providing: (i) government services, (ii) services which are provided by private organizations to the Government of Indonesia, and (iii) specific services which are identified to be strategic by sectoral regulators. It would then be up to the specific sectoral regulators to publish specific lists of services which are strategic, instead of the proposed overly-broad categories in the current Article 5(1a)(c).** We also understand that the registration procedure for electronic system operators will be governed under Ministerial Regulation. We recommend that the procedure be light touch to avoid imposing unnecessary costs and burdens on businesses (local and foreign alike), with no physical presence or local infrastructure being required. For instance, registration could be completed and updated online without manual checking. We also recommend that the registration under this procedure should be granted as a matter of course where the electronic system operator in question meets the requirements for registration; and that the procedure should not include any discretion to withhold registrations. The Draft Amendment also states that electronic system operators will have one year to comply with the amended GR82 (after the amendments go into effect). We recommend that the Ministerial Regulation be issued in timely manner so that businesses would

		have adequate time to comply with the one-year transition period, particularly for existing systems.
Article 15 - Removal of electronic information and/or document *'15(A)(1)- All Electronic System Operators are required to delete irrelevant Electronic Information and/or Electronic Documents that are under their control based on the request of the relevant Person based on a court order; (2)- Electronic System Operators that are required to delete the Electronic Information and/or Electronic Documents* as referred to in *paragraph (1) are Electronic System Operators that gain and/or process Personal Data under their control.* *(3)- Except if there is a provision in the Law that regulates the Electronic Information and/or Electronic Document that requires the said information or document to be kept or that forbids the said information or document to be deleted, the provision as referred to in paragraph (1) is invalid.'* *'15(B) The irrelevant Electronic Information and/or Electronic Documents as referred to in Article 15A paragraph (1) include Personal Data that:* *f. are displayed by the Electronic System Operator that cause losses for the owner of the Personal Data.'* *'15(D)(1) Every Electronic System Operator is required to provide a deletion mechanism for deleting irrelevant Electronic Information and/or Electronic*	We suggest that the deletion of electronic information / documents upon request by individuals in **Article 15A** should be subject to certain reasonable exceptions, such as when the information/documents in question: a. are or have become publicly available; or b. are still required to be retained, processed, disclosed and/or otherwise used by the electronic system operator for any one or more of the following purposes: i. Establishment, exercise or defense of legal claims and rights. ii. Investigations and/or fraud prevention. iii. Compliance with legal obligations. iv. Performance evaluation. v. Public interest (including public health) purposes. vi. Scientific or historical research. vii. Statistical purposes. We also recommend that: • **Article 15B(f)** should be omitted for the reasons provided in the right column; • In relation to the ability for sectoral regulators to prescribe the deletion mechanism for their respective sectors **Article 15D**, it should be clarified that: o sectoral regulators must still incorporate the safeguard that a court order is needed before the electronic system operator can be required to delete the information/documents in question, and also the various factors for the court order to be awarded; and	We support the requirement that an individual must obtain a court order to request an electronic system operator to delete electronic information and/or documents pertaining to the individual. This is an important safeguard against abuse by individuals seeking to delete information that the electronic system operator in question may legitimately need to retain. For example, if an individual is under investigation or is involved in a dispute, that individual should not be allowed to abuse this right of deletion to require an electronic system operator to delete incriminating or relevant information that relates to the investigation or dispute. Individuals should not be allowed to abuse this right to request electronic system operators to delete invoices which are presented to the individual, and debts which are owed by the individual. Individuals (who are employed by companies) should also not be allowed to abuse this right of deletion by requiring their employer to delete negative performance reviews because of their poor performance. However, we also note that proposed **Articles 15A – 15D** are silent on the factors that the court should take into account when awarding the court order for the electronic system operator to delete information/documents. We therefore recommend that the Draft Amendment include at the minimum the factors identified in the middle column of this table. We would be happy to work with KOMINFO to identify the appropriate factors but at a minimum these should include the points mentioned be made exceptions to the right of deletion. **Article 15B(f)**, which, in effect, allows for the removal of electronic information and electronic documents "which results in harm to its owner" is overbroad. Such a broad definition of "irrelevant data" will skew the

Documents requested by the relevant Person. *(2) The deletion mechanism as referred to in paragraph (1) should at least contain provisions on:* *a. court order document;* *b. internet address/uniform resource locator (url) or other format that shows the location of the irrelevant Electronic Information and/or Electronic Document display; and* *c. irrelevant Electronic Information and/or Electronic Documents to be deleted, including the display.* *(3) Data collection as referred to in paragraph (2) point b includes:* *(4) Further provisions on the deletion mechanism as referred to in paragraph (1) to paragraph (3) are governed by the Ministerial Regulation.* *(5) Provisions on deletion mechanism/s in certain sector/s can be formulated by related Sectoral Supervisory and Regulatory Institution after coordination with the Minister.'*	○ if an electronic system operator is required by a sectoral regulator to comply with a sector-specific deletion mechanism, then the electronic system operator has the option of not implementing the general mechanism under GR82 and instead using the sector-specific deletion mechanism for other non-sectoral requests for deletion of information/documents; and • **Article 15D(3)** should be deleted as it appears to be incomplete and erroneously included.	proper balance between data protection on one hand, and free speech and the Indonesian citizens' right to information on the other. It could be argued that the harm sought to be addressed by Article 15B(f) is already addressed by Indonesia's criminal laws on defamation and its civil laws on tort. The public's right to access lawful information should not be compromised by provisions such as Article 15B(f) which may allow overbroad authorization to permit the deletion of information which are of public interest. However, if there are strong sentiments for retaining **Article 15B(f)**, it should be qualified to ensure that the deletion of the data sought to be removed by the data owner will not negatively impact the public interest or the public's right to information (especially if the data involves important information about persons who represent them in government or provide them services). We also note that proposed **Article 15D** allows sectoral regulators to prescribe the deletion mechanism for their respective sectors, and have recommended a few clarificatory amendments.
Article 83C - The role of the government to facilitate the use of information technology and electronic transactions in infrastructure facilitation. '*Infrastructure facilitation as referred to in Article 83B point c includes:*	In relation to **Article 83C.f**, we recommend omitting the reference to "source code temporary keeping or storage". Alternatively, we recommend further clarification on what is envisaged by this reference.	Mandatory source code disclosures could significantly undermine the protection of trade secrets and other intellectual property of domestic and foreign technology companies. We therefore recommend the deletion of the reference to "source code temporary keeping or storage" in proposed Article 83C(f). Alternatively, we would like to request for clarification on what would be envisaged by this reference.

f. source code temporary keeping or storage and documentation of software applications for institutions; and		
Article 83K - Classification of data that must be on shore *'(1) The types and scopes of strategic electronic data that are mandatory to be protected as referred to in Article 83J are those that meet the criteria that any threat and/or disturbance to them will cause:* *a. disaster to humanity and development;* *b. national transportation and/or communication chaos;* *c. disturbance of government activities;* *d. disturbance of law enforcement process;* *e. disturbance of defense and security;* *f. disturbance of national economic security; and/or* *g. other criteria based on provisions in the legislation'.* *'(2) Types and scopes of strategic' electronic data that are mandatory to be protected as referred to in paragraph (1) are identified by the Sectoral Supervisory and Regulatory Institutions, Agencies, and/or institutions by paying attention to the characteristics of legal protection need and the strategic nature of the Electronic System operation.'*	We recommend that the definition of "Indonesian citizen data" does not include personal data obtained by electronic systems providers based on customer consent for the purpose of providing services. We also recommend: a. clarifying the scope of "strategic electronic data" to only cover data for true critical information services (like public utilities) and to allow an exception for data recovery centers to be located outside of Indonesia (or in the cloud) if the data is not critical to national security or the provision of basic telecommunications, water, or electricity services; b. amending the proposed revised **Article 17** and proposed **Article 83L** to allow data recovery centers to be located outside of Indonesia (or in the cloud); and c. providing an explicit exception for electronic data that is necessary to facilitate the lawful sale, purchase, and/or delivery of a good or service We also suggest the following revisions to the text of the **Article 17** to implement recommendations b. and c. above: "**Article 17** – '3. Provisions in paragraph (1), paragraph (2), and paragraph (3) of Article 17 are amended that Article 17 becomes as follows:	We welcome the clarification on data which must be located on shore and what is acceptable to be located offshore. While we agree with the list of criteria for "strategic electronic data" in Article 83K, the explanation to Article 83K mentions that "strategic electronic data" includes "demographic data or Indonesian citizen data". This unfortunately and unnecessarily broadens the definition of "strategic electronic data". It cannot be the intention that Indonesian personal data that is processed by an Electronic System Operator cannot leave Indonesia in all instances. There are situations where it is necessary for Indonesian personal data to leave Indonesia. As identified above, an Electronic Systems Operator that provides public services may process personal data of Indonesian citizens outside of Indonesia for very legitimate and necessary reasons (for example, when the transaction relates to a cross-border transaction, and in relation to fraud prevention purposes). In addition, there are technical and architectural reasons why many of the services in this category could foreseeably suffer from resiliency and availability constraints as more apps become cloud native and workloads require multiple geographic instances to guarantee up-time. By limiting the movement of data, the policy could require something in the order of three times the investment in local cloud capability to achieve a relative level of service availability We thus recommend that the definition of "strategic electronic data" should not include "demographic data" or "Indonesian citizen data". Instead, and in line with our recommendation in the cover letter to exclude matters of personal data protection from the ambit of GR82, any restrictions on where personal

'(3) Agencies and/or institutions that own strategic electronic data that are mandatory to be protected based on the results of identification as referred to in paragraph (2) submit a request to the Minister to be assigned as the agency or institution that owns strategic electronic data that are mandatory to be protected.' *'(4) In addition to strategic electronic data as referred to in paragraph (1), agency and/or institution can assign high electronic data and low electronic data.'*	b. Electronic System Operators are required to have a business continuity plan to mitigate disturbance or disasters according to the risk/s of the impact/s produced. c. Electronic System Operators for public services are required to place and process strategic electronic data in a data center and disaster recovery center in areas of Indonesia **or to demonstrate they have the capacity to back-up and replicate all data in the event of a disaster. Electronic data that is necessary to facilitate the lawful sale, purchase, and/or delivery of a good or service is not deemed to be strategic electronic data for the purposes of this section.** We also seek clarity on whether it will be up to individual regulators to determine the definition of "strategic data." If so, we seek clarity on whether each individual regulator will be required to explain to the Ministry why it is using a particular definition for strategic data. We also seek clarity on whether a particular regulator will be required to apply to the Ministry to classify certain types of data, for example payments data, as strategic data. We recommend that that the concepts of "high electronic data" and "low electronic data" be merged into a single concept of "other electronic data" as there appears to be no difference in the legislative treatment of the "high electronic data" and "low classes of data. Lastly, we seek clarity on whether existing Bank of Indonesia (BI) regulations that call for data onshoring will be retroactively reviewed. These regulations	data can or cannot be used, processed, and/or stored should be left to the omnibus personal data protection legislation that the Government of Indonesia is contemplating. This will provide for a clearer definition of "strategic electronic data". Proposed **Article 83K(2)** appears to contemplate that sectoral regulators have the ability to define what falls within the scope of "strategic electronic data". We recommend that, in order not to have differing interpretations of what falls within the scope of "strategic electronic data", the Draft Amendment should incorporate a requirement for sectoral regulators to apply to KOMINFO for approval for the types of data (e.g., payments data) they want classified as "strategic electronic data", and for KOMINFO to consult affected electronic system operators or the public before granting the approval. There does not appear to be a difference in the legislative treatment of "high electronic data" and as compared to "low electronic data" (other than the different definitions in the explanatory notes at the back of the Draft Amendment). If there is not intended to be a difference in legislative treatment, we recommend that the concepts of "high electronic data" and "low electronic data" be merged into a single concept of "other electronic data". This will further streamline the drafting of GR82 and simplify compliance. If there is intended to be a difference in the legislative treatment of the two classes, we recommend that the Draft Amendment should include additional provisions to clarify the difference.

	include: Circular 17/52/DKSP; PBI 18/40/2016 and PBI 19/10/2017.	
Article 83P - Requirement to backup and connect strategic data into centralized data centers for security purpose	We seek clarification on how 'connectivity' to the national data center and national data recover center for strategic electronic data will actually be implemented in practice	
Article 84 (as proposed in the Draft Amendment) - Administrative sanctions	It is unclear what "access" may be terminated under **Article 84(2)(d)**. We would be grateful for clarification on this.	
Article 8 of GR82 - Requirement for mandatory source code disclosure	We recommend removing Article 8 of GR82, which could significantly undermine the protection of trade secrets and other intellectual property of domestic and foreign technology companies.	
On Personal Data/ Data Privacy, there are provisions in GR82 that regulate how personal data is to be collected, handled, and disclosed by electronic system operators.	We recommend removing all provisions relating to personal data and leaving matters of personal data protection to be regulated by the omnibus personal data protection law that Indonesia has been considering.	This would result in a clearer regime for personal data protection in Indonesia, which would in turn create a more certain legal environment for businesses to operate in Indonesia.