Recommendations on Indonesia's Personal Data Protection Bill

1 April 2019

His Excellency Rudiantara
Minister of Communications and Information Technology
Ministry of Communications and Information Technology of the Republic of Indonesia
Jalan Medan Merdeka Barat No. 9,
Jakarta 10110
Indonesia

Dear Minister Rudiantara,

We are writing to express our sincere gratitude to the Ministry of Communications and Information Technology ("**KOMINFO**") and the Government of Indonesia to submit comments on the Law of the Republic of Indonesia on Personal Data Protection ("**the Bill**").

We appreciate the government's efforts to protect personal data and value this opportunity to provide the following recommendations to ensure that the Bill achieves its vision for data protection and privacy in Indonesia, while continuing to allow for innovation and the growth of Indonesia's digital economy.

1. Clarifying definitions

Maintaining consistency across jurisdictions provides greater clarity to companies operating in multiple countries. In the interest of providing clear, effective guidance to multinational companies, **definitions used in the Bill (e.g., for "Personal Data" and "Processing") should be consistent with international practice**.

Relating to the definition of "Personal Data", we further recommend that the scope of data covered under the Bill should pertain to personal data that, if mishandled, would have a meaningful impact on a consumer's privacy. Accordingly, the definition of "Personal Data" and the Bill should exclude data that is anonymized or de-identified through robust technical and organizational measures to reasonably reduce the risk of re-identification.

2. Clarifying the roles and responsibilities of data controllers and data processors

In addition to clarifying definitions, we strongly recommend that the Bill **clarify the roles and responsibilities of Data Controllers and Data Processors**. Data processors and data controllers have very specific roles in the data lifecycle with differing visibility and degrees of control over the decisions for collecting and processing personal data. It would also be difficult, if not impossible in many cases, to effectively implement a data protection framework that places the same responsibilities on both data processors and data controllers, especially in situations where data processors have no visibility as to the nature and content of the data that they are processing on behalf of data controllers.

Modern data protection laws such as the EU GDPR and the Philippines Privacy Law make a very clear distinction between the roles of the data processor versus the data controller, and we strongly recommend that similar clarity and distinction in the Bill. In particular, the data processor should be responsible for complying with the lawful instructions of the data controller, and for the harm suffered by the data subject if the data processor acts outside of such instructions.

3. **Adding exceptions and limitations to the rights of Personal Data Owners**

We recommend that the **Bill include exceptions and limitations to the rights of Personal Data Owners similar to the GDPR**. These would include exceptions and limitations to what companies have to provide to consumers, what personal data has to be deleted, what personal data must be restored, what access must be given, and personal data owner's "right to be forgotten."

4. **Expanding exceptions to personal data protection**

We also strongly recommend that the **exceptions to personal data protection under the Bill should be expanded in line with international practices**. These exceptions should include, among others, processing of personal data:

(a) for scientific or historical research purposes or statistical purposes;
(b) for journalistic purposes;
(c) for the purposes of academic, artistic or literary expression; and
(d) by a natural person in the course of a purely personal or household activity.

5. **Extra-territorial scope**

The Bill applies to every Person, Public Authority, Business, and organization/institution "both within the Indonesian jurisdiction and outside Indonesian jurisdiction, with legal consequences within the Indonesian jurisdiction and/or outside of Indonesian jurisdiction and harms the interest of Indonesia". This provision is extremely broad and seems to amount to Indonesia seeking to exercise extra-territorial effect on entities across the world, which would not be enforceable.

To ensure that the Bill is effective and achieves its objectives of protecting Indonesian data subjects, **it should be limited to governing conduct that has a sufficiently close connection to Indonesia**. In relation to this, we recommend that the scope of the Bill should be amended to apply only where: (1) residents of Indonesia are specifically targeted; (2) the personal data that is the object of the processing is purposefully collected from data subjects in the country at the time of the collection; and (3) such collection is performed by an entity established in the country through a stable arrangement giving rise to a real and effective level of activity.

6. **Ensuring transfers of personal data cross-borders**

The Bill should provide for **several standalone bases on which transfers of personal data outside of Indonesia are permitted.** This would bring the regulation in line with international practices, such as those under the EU GDPR, as well as other regional privacy laws such as in the Philippines, Malaysia and Singapore.

We strongly emphasize that the free flow of data across borders confers multiple benefits for economies and the financial services ecosystem. Open markets, and the ability to move data relatively freely across national borders, have helped facilitate a number of innovative developments over the past decade. These advances include cloud computing and ongoing progress with Smart Cities and the Internet of Things (IoT). Such developments have conferred significant economic benefits, including productivity gains, lowered costs for consumers, and increased employment. As electronic commerce continues to grow and digital technologies become ubiquitous, the ability of organizations to easily share data across borders becomes even more essential.
Free cross-border data flows also enable entrepreneurs in developing regions to take advantage of the data infrastructure outside their home countries. This helps bring new and/or enhanced services to local consumers and businesses.

Additionally, we would like to reiterate the importance of cross-border data flows to economic growth and development. Rapid advances in technology have changed the way business is conducted around the world. As a 2017 study by the Information Technology & Innovation Foundation (ITIF) notes, global digital trade is increasing rapidly and thus spurring economic growth, driven by increasing usage of cloud-based internet services. With digital trade and cross-border data flows expected to grow faster than the overall rate of global trade, any impediments to data movement can have profound consequences for economies.

7. **Remove Criminal Penalties from the Bill**

A central regulator should have the tools and resources necessary to ensure effective enforcement. However, remedies and penalties should be proportionate to the harm resulting from violations of data protection laws. Criminal penalties are not proportionate remedies for violation of data protection laws, would be inconsistent with internationally-recognized best practice, and are likely to chill legitimate data processing activities. We therefore recommend the removal of all criminal provisions from the Bill.

8. **Ensure manageable transitional provisions for the implementation of the Bill**

We strongly recommend that parties be allowed at least **two (2) years** to comply with the provisions of the Bill. We further recommend that personal data that have been collected and/or processed by data controllers and/or data processors (under and in compliance with existing applicable regulations) should be excluded from the scope of the Bill.

Please also find attached to this letter a matrix, which explains our concerns in greater detail, seeks clarification on several provisions, and offers further recommendations for refining the Draft Bill. **We would like to respectfully request that KOMINFO and all other relevant agencies consider these detailed comments and recommendations when reviewing the draft Bill.**

We thank you again for conducting an open and transparent consultation process as you seek to further develop an effective regulatory approach to personal data protection in Indonesia. We believe that there are great opportunities for industry and the Government of Indonesia to work together on developing and implementing such an approach. We look forward to further, closer collaboration to ensure that both national and individual interests are protected, and that Indonesia remains an attractive, enabling environment for innovation, security and the growth of the digital economy. U.S. industry is committed to supporting Indonesia in achieving its vision for safety and advancement in the digital economy, particularly in shaping this important legislation to support this vision. It is of vital importance that policies that address personal data protection in Indonesia are aligned with global best practices to ensure Indonesia remains a global hub for growth and investment in the data ecosystem. Our respective members are global leaders in ICT and have experience and expertise on how to manage personal data effectively and safely.

Our organizations and our respective members stand ready to work with the Government of Indonesia to further improve the Bill and ensure the protection of personal data in Indonesia. We hope that our input will be useful to improve the current Bill and we would welcome a meeting with KOMINFO to further discuss our concerns.

We thank you for considering our views.

Sincerely,

Alexander C. Feldman
President & CEO
U.S.-ASEAN Business Council

Darryn F. Lim
Director, Policy – APAC
BSA | The Software Alliance

Attachment

cc: Iwan Susanto, Charge d'Affaires Embassy of Indonesia in Washington, D.C.
The Honorable Joseph R. Donovan, Jr., United States Ambassador to Indonesia

Attachment

Corresponding Chapter in the Bill	Corresponding Articles	Comments	Recommended Revision
I on General Provisions	1 - 2	Maintaining consistency across jurisdictions provides greater clarity to companies. In the interest of providing consistent, effective guidance to multinational companies, definitions such as those used in the GDPR should be adopted. The GDPR defines "personal data" as: "any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly (GDPR Art. 4(1)), in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (GDPR Art. 9(1)) We appreciate the Government of Indonesia's efforts to protect personal data in order to ensure the security and personal protection of the public. We are committed to supporting these efforts. However, the definition is too broad and needs to be narrowed down. The definition of "Personal Data", when read with Article 1.6, appears to extend beyond data of individuals and also cover data of corporations. Privacy issues with these two different types of data are often different and should be addressed by different rules. The "Personal Data" definition would also be improved if identification of the person was by	**Article 1.1** We recommend amending the definition of "Personal Data" to confine it to data that relates to an identified or identifiable natural person (and not include any data that relates to corporations or organizations). **Article 1.2** We recommend streamlining the terminology used throughout the Bill to either "data" or information". Article 1.2 should be amended accordingly. **Article 2** We recommend amending Article 2 to clarify that the law only applies where: (1) residents of Indonesia are specifically targeted; (2) the personal data that is the object of the processing is purposefully collected from data subjects in the country at the time of the collection; and (3) such collection is performed by an entity established in the country through a stable arrangement giving rise to a real and effective level of activity.

		means likely to be used by the data controller/processor. **<u>Article 1.2</u>** It is also unclear what is the difference between "data" (used in Article 1.1) and "information" (Article 1.2). The terminology used throughout the Bill should be streamlined to either "data" or information". **<u>Articles 1.6, 1.10, 1.11</u>** The concepts of "corporation", "Person", "Business Actor" and "organization" are overly complex. There is also inconsistent use of these terms in the law (e.g. in Article 2, the terms "Business Actor" and "organization / institution" are used, but in Article 77, the term "Corporation" is used). The terminology should be rationalized. **<u>Article 2</u>** Article 2 is very vague and implies a scope so wide that the law would not be administrable by businesses and would be in conflict with other jurisdictions. It talks about entities that perform legal acts in accordance with the law in Indonesia or outside Indonesia with legal consequences in Indonesian jurisdiction or ones detrimental to Indonesian interests if outside. To ensure that the Bill is effective and achieves its objectives of protecting Indonesian data subjects, **it should be limited to governing conduct that has a sufficiently close connection to Indonesia**.	
II on Norms, Principles and Objectives	3 - 5	The principles laid out here are very prescriptive and not clearly defined. It is not clear what the criteria are for terms such as "accurately", "completely", "limited and specific manner", "non-misleading and up-to-date".	**<u>Article 4 paragraph c</u>** We recommend deleting paragraph c of Article 4 in its entirety

		Article 4 sets out the general principles and these are partially reiterated in Articles 37, 38 and 39. This is largely a sensible list, though it also includes two 'principles' that seem to imply primacy for consent – the first of several occasions where the grounds for processing are apparently contradictory. In addition, the definition and timeline for retention is never made clear nor is it clear how a data processor treat or destroy data post-retention period.	
III on Types of Personal Data	6	Article 6 further subdivides "Personal Data" to "General Personal Data" and "Specific Personal Data". The language in the article is very awkward and unclear but the explanation at the back of the document provides examples such as name, gender, nationality, religion and other identifying info for general and health records, biometric data, genetic, sex life, politics, criminal record, children's data and personal financial data for specific. In other words, it largely maps to sensitive data in other jurisdictions. Other than financial data, which is rarely considered in the sensitive category in other jurisdictions, these examples should be moved into the body of the Articles as a definitive list of what constitutes "Specific Personal Data". "General Personal Data" can then be simply defined as all "Personal Data" that is not "Specific Personal Data".	We recommend moving the examples in the explanatory section for "Specific Personal Data" into the body of the Articles as a definitive list, and excluding financial data which is rarely considered in the sensitive category in other jurisdictions.
IV on Personal Data Owner Rights	7 – 18, also related to 34-41 and 61	Similar to GDPR, there should be exceptions and limits to each of these rights. Articles 7 – 18 set out the rights of data owners. Some of these are further elaborated in Articles 34 – 41. These are fairly wide, along the lines of EU GDPR. One strange one is the right to "choose"	**Articles 7, 8, 13, 14, 16** We recommend deleting Articles 7, 8, 13, 14 and 16 in their entirety. **Article 9** We recommend including the following safeguards/limitations to the right under Article 9:

		pseudonymization for "certain purposes" (Article 14). It is not clear where and when this applies. Also, Article 27 gives data controllers 3 days to stop processing data for which consent has been withdrawn. This is unrealistic. We suggest expanding Article 27 to be a general obligation to respond to data owner requests inside 30 days. **Article 7** Article 7 is vague. Data controllers would be challenged to respond to such requests and yet remain compliant with the rest of the law. **Articles 8, 14, 17** These rights should be removed as they are already addressed in substance by other provisions in the Bill. **Article 9** There should be limits on what organizations have to provide (e.g., organizations should not have to search unstructured data sources (emails, metadata); costs incurred should be relevant; organizations should be able to verify the personal data owner's identity before responding). We also propose clarifying the concept of "suspension of data processing", for example, what activities will fall under this provision. **Articles 11, 12, 27, 39, 40, 41, 61** The right to deletion/destruction is too absolute and not in line with international norms and best practice in other countries. The deletion/destruction of data may not be feasible or desirable in certain circumstances. The Government of Indonesia should consider carefully redrafting the law such that the public will not use this rule to egregiously delete	• limits on what companies have to provide (e.g., we should not have to search unstructured data sources (emails, metadata); • costs incurred should be relevant; • companies should be able to verify the personal data owner's identity before responding) The concept of "suspension of data processing" should also be clarified. **Articles 13, 34, 35** We recommend deleting Articles 13 and 34 in their entirety, and including a sub-paragraph d. in Article 35 as follows: ***Article 35*** *Personal data controllers must refuse to give access to changes in Personal Data to Personal Data Owner if:* *a. it endangers the physical security or health or mental health of individuals other than the Personal Data Owner;* *b. it leads to a disclosure of Personal Data belongs to other person; and/or* *c. it is contradictory with national defense and security interests.* ***d. It cannot be validated/verified according to relevant legal, medical or other documentation available to Personal Data Controller.*** **Articles 11, 12, 27, 39, 40, 41, 61** We recommend deleting Articles 11, 12, 27, 39, 40, 41 and 61, which relate to the right to be forgotten. **In the alternative,** we recommend amending Article 61 as follows:

		information relating to that individual on the internet or on any form of public domain and against public interest. For example, data aggregators often collect personal data that is available in the public domain. There could be positive use cases such as personal data of lists of sex offenders, convicts, wanted individuals or fugitives that are publicized to warn the society of the dangers surrounding these individuals. Given the above, there should be an exception such that data aggregators are not subject to obligation to delete personal data upon a data owner's request. Ideally, there should be higher standards on the conditions that would trigger the right to be forgotten, so that it would not hinder the flow of information and the public basic rights for access to useful and accurate information. There should also be an opportunity for the data controller to defend its case against users requesting the court to issue a court order to remove its information. Otherwise, this one-sided process can be used abusively by the users. We also recommend some reasonable exceptions for the deletion of personal data, such as when the information still needs to be stored, processed, disclosed, and / or used by organizations for the following purposes: i. Implementation or defense of legal rights ii. Investigation and / or prevention of fraud iii. Adjustments to legal obligations, including the obligations of life insurance companies to carry out their obligations under the insurance policy	***Article 61*** *(1) Business Actors Association can develop a Personal Data Controller Conduct Guideline.* *(2) In developing the Personal Data Controller Conduct Guideline as referred to in paragraph (1), the Business Actor Association must consider:* *a. Personal Data processing purpose;* *b. principles of Personal Data Processing; and* *~~c. input from Personal Data Owners or their representative Associations.~~* ***(3)** The Personal Data Controller Conduct Guideline must have the same level of protection as stipulated in this law ~~or higher,~~ **unless otherwise regulated by Sector Supervisory and Regulatory Agencies.*** *~~(4) The Personal Data Controller Conduct Guideline may not conflict with this Law.~~* **Article 16** We recommend amending Article 16 to clarify that the quantum and award of compensation is subject to the applicable court process. **Article 17.1** We recommend including and specifying clear criteria in Article 17.1. **Article 17.2** We recommend deleting Article 17.2 or specifying clear criteria.

		iv. Performance evaluation v. Objectives of public interest (including public health) vi. Scientific research vii. Statistical goal Also, the data removal clause will prevent blockchain being rolled out in Indonesia since, due to the inherent way the technology works, blockchain records can never be removed. We do not believe that KOMINO wants the unintended consequence of restricting future digital growth in Indonesia through preventing blockchain. In the context of life insurance, the personal data of the customer is very important and is the basis for the insurer to carry out its obligations under the insurance policy, which are paying health, life, or other insurance benefits. The deletion/destruction of customer data will prevent the insurer from being able to pay claims, considering that the validation of claims and customer information needs to be done before paying the claim, and customer-related information is also needed to carry out payments. It will also prevent insurers from conducting fraud investigation or defending a litigation, and this would be the case for both active and non-active customers. If insurers are unable to retain data, the undesirable consequence would be that customers do not get insurance protection because insurers cannot give services to the customer. This can also be counter-productive to financial inclusion and the growth of the financial industry, which is part of the Government of Indonesia's strategic plan. **Articles 13, 34, 35**	**Article 18** We recommend adding a qualifier to the effect that where requests from a data subject are manifestly unfounded, unduly burdensome or excessive (e.g., because of repeated requests), the data controller may either: a. charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or b. refuse to act on the request. The Data controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

		It needs to be clarified what it is meant by giving access, considering that in granting access to its system to one customer, an organization must also consider the personal data of other customers, its own organization data and the capabilities of its systems. We are of the view that a "providing information" approach is more appropriate. This would still meet the same objective of ensuring that data owners are able to know what personal data of theirs are stored and managed by the data controller. On data modification, considering the importance of the accuracy and validity of data in financial institutions, especially life insurance companies, we propose that data controllers should be permitted to reject requests for modification of personal data in the event that they are not in accordance with relevant legal documents. Furthermore, mandatory data verification is still carried out by applying high standards to ensure data accuracy, before making any modification. On data profiling, this is often needed to provide good service for customers, namely by maximizing and targeting customer service in accordance with the needs of customers and profiles of each individual, while remaining in line with customer agreement and statutory provisions, especially regarding confidentiality. Therefore, we propose that there should be flexibility for organizations to implement data profiling in the conduct of their businesses **by removing the provisions of Article 13**, subject to Article 58 related to profiling agreements.	

		Article 16 The provision states that the data owner is entitled to sue and receive compensation in the event of personal data breaches. It should be clarified that the quantum and award of such compensation should be subject to the applicable court process. **Article 17** This Article should take into account the structure and storage format of the personal data that was originally received and processed without imposing unreasonable and excessive cost on Personal Data Controllers. That is, the rights under this Article should apply only where the personal data is received and processed by electronic means and readily-available in a structured and commonly used format. Conversely, where the personal data is obtained in hardcopy format, in a format that is not commonly used or not in a machine-readable format, data controllers should not be required to expend excessive and unreasonable efforts to comply with the request. **Article 18** There should be a safeguard against requests from data owners that are manifestly unfounded, unduly burdensome or excessive (e.g., because of repeated requests),	
V on Private Data Processing	19 - 23	In the interest of providing consistent, effective guidance to multinational companies, definitions such as those used in the GDPR should be adopted. The GDPR defines 'processing' as: "any operation or set of operations which is performed on personal data or on sets of	**Article 20** We recommend adding another ground for data processing in Article 20 – where processing is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party".

		personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction," and "pseudonymization," defined as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." (GDPR Art. 4(5)). **Article 20** Article 20 is the first attempt to set out the lawful grounds for processing personal data but it pops up again in many places. The grounds include performance of contract, legal obligation, vital interest, public interest and "legitimate agreement by Personal Data Owner". However, it should also recognize and enable the processing of personal data for legitimate business interests (e.g., cybersecurity efforts, detecting or preventing fraud or identity theft, exercising or defending against legal claims, to name a few), and other purposes that are consistent with the context of the transaction or expectations of consumers. **Article 21** On breach of personal data, there needs to be clearer provisions on what is considered as failure to protect personal data and what are the thresholds for	**Articles 20, 21, 22, 25** We recommend including the following exceptions to Articles 20, 21, 22 and 25: a. opinion data kept solely for an evaluative purpose; b. any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results; c. the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust; d. personal data kept by an arbitral institution or a mediation center solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation center; e. a document related to a prosecution if all proceedings related to the prosecution have not been completed; f. processing of personal data necessary for: a. exercising of the right of freedom of expression and information; b. compliance with a legal obligation; c. performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, including on the grounds of public interest in the area of public health; d. archiving purposes in the public interest; e. scientific or historical research purposes or statistical purposes; or f. the establishment, exercise or defense of legal claim.

		data breach; for example, as is the case in Australia, if the data breach would cause serious physical, psychological, emotional, economic, reputational, and financial harm. It also appears that all consent under the law must be recorded in some medium. The standard for determining the level of consent that is appropriate should be contextual. In circumstances that do not implicate heightened sensitivity, implied consent may be appropriate. It would therefore be good for the law not to preclude implied consent (where consent can be implied from the surrounding circumstances). **Article 21(4)** More clarity needed on how to "distinguish" the request for consent. **Article 22** Article 22 adds grounds for "Specific Personal Data" – though it is phrased as maintaining confidentiality rather than processing per se, so it's not clear where the border between Articles 20 and 22 lies for specific personal data. **Article 23** Article 23 covers the grounds for using visual data processing equipment in public spaces. It is, however, unclear how this Article ties in with the restrictions/permissions for data processing in Articles 20, 22 and 25, among others (which as noted in our comments to those articles, also appear to be in conflict with each other). For example, it is unclear if the Article 23 requirements are in addition to the grounds under Article 20 or instead of those grounds. If the latter, it is a little limiting in terms of use cases (e.g. retail analytics, patient observation).	**Article 21** We recommend including clearer provisions in Article 21 on what is considered as a failure to protect personal data and the thresholds for data breach. **Article 21(4)** We recommend amending the Bill to include more clarity on how to "distinguish" the request for consent. **Article 22** We recommend amending the Bill to clarify how Article 22 interacts with Article 20. **Article 23** We recommend amending the Bill to clarify the relationship between Article 23 and the restrictions/permissions for processing in Articles 20, 22 and 25, among others. We also recommend including more clarity/detail as to whether Article 23 would permit workplace applications for visual data processing. **Article 25** We recommend deleting Articles 25.1 and 25.3, and converting Articles 25.2 and 25.4 into general information obligations. Additionally, with respect to Article 25.2, we recommend including only information relevant to the collection, use, or disclosure of personal data. All other information to be provided (e.g. retention period) should be deleted.

		In addition, more clarity on workplace applications for visual data processing is needed. **Article 25** Article 25 contradicts Article 20. Article 25 appears to require consent as the default grounds for processing (as compared with Article 20 where consent is an alternative ground for processing). Additionally, the exceptions included in Article 25 – life-threating situation, legal obligation, health services, judicial process, legal function, public domain (specific personal data), legal obligation, perform contract - roughly equate to the provisions under Article 20 but it is unclear why two different and conflicting versions have been included. Further, the information required to be given in Article 25.2 for there to be valid consent should focus on the purposes for the collection, use of disclosure of personal data. All other information to be provided (e.g., retention period) should be a separate obligation, and not a condition to a valid consent.	
VI on Obligations of Personal Data Controller, Personal Data Processor, and Third Party Processors in Personal Data Processing	24 - 48	**Article 25, 27, 39-41** This section merits clarification, particularly on the 'details regarding Information collected'. Articles 39-41 could be problematic if consumers can select pieces of data to delete. As an example: The concept of personally identifiable information is complex, and it is critical that the data a consumer receives be meaningful and understandable to the consumer. Giving that person a long list of data elements diminishes this meaning, and is also very difficult for the operator to provide. Similarly, requiring the provision to a consumer of the names	**Articles 25, 27** We recommend changing the time frames in Articles 25 and 27 to "within a reasonable amount of time in light of the applicable circumstances". **Article 26** We recommend clarifying how the consent required under Article 26 may be 'displayed' and also what exceptions would apply to the requirement to display consent. **Article 28**

		of third parties that receive the consumer's personal data fails to appreciate the complexity of the online ecosystem, and as currently drafted this provision would fall far outside the mainstream. It is much more feasible and meaningful to the consumer if the operator can provide categories of third parties. There are also costs associated with this requirement as most systems are not configured to track and report back to individuals each specific entity that may have access to the consumer's data. **Article 25.4** Subject to our earlier comments above on Article 25, the timeframes in Article 25.4 should not be tied to an arbitrary timeframe of 7 days. **Article 26** It is unclear how this obligation is to be fulfilled. This needs to be clarified. Furthermore, there may be situations where it would be impracticable or not legally possible to "display the consent" (e.g., where the consent was given in a private agreement that is protected by express confidentiality obligations). **Article 27** The three-day timeline is unreasonable as there is generally a multi-step process required for organizations to stop processing and confirm it. The timeline for withdrawal should be at least 30 days from the date the withdrawal request is accepted of withdrawal and the Bill should provide specific details on the requirements for withdrawal request responses, along with a timeline for that process. **Article 28** This provision is unclear, and it is not practical to implement.	We recommend deleting Article 28 in its entirety. **Article 29a** We recommend amending Article 29a to read as follows: "Personal Data Controller must protect and ensure the security of the Personal Data in its possession or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks." **Article 33** We recommend amending Article 33 to read as follows: "Each Data Controller shall maintain records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data. Records should include: a. Information about the purpose of the processing of personal data, including any intended future processing or data sharing; b. A description of the general categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing. **c.** General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data."

		Article 29a It is unclear what it means to protect personal data from disruption of personal data processing. **Articles 29 – 32** Articles 29 – 32 provide general obligations for the data controller to undertake technical and organization security measures according to the risk. This is welcomed and should be extended to data processors. However, more clarity on the "technical steps" that data controllers should take is needed, bearing in mind that some such steps could be proprietary. **Article 33** This obligation is overly broad and could impose an undue burden that is costly and impractical on all parties operating in Indonesia, without a clear data protection outcome. The obligation to maintain records should be primarily on the data controller who has visibility into the purpose for which the personal data is collected and processed. The data processor often will not have knowledge of the purpose. Moreover, this requirement should be limited to specific categories of information that have a clear link to a data protection outcome for example, the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; where applicable the categories of recipients to whom the personal data may be disclosed. There should also be an exemption for small / medium enterprises for whom such a requirement would pose an economically infeasible obligation. This is recognized in the GDPR, which provides an	**Article 34** We recommend deleting Article 34 in its entirety. **Article 36.1** We recommend amending Article 36.1 to read as follows: "The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. This provision will not apply to a. opinion data kept solely for an evaluative purpose; b. any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results; c. the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust; d. personal data kept by an arbitral institution or a mediation center solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation center; e. a document related to a prosecution if all proceedings related to the prosecution have not been completed; f. personal data necessary for: a. the exercising of the right of freedom of expression and information; b. compliance with a legal obligation; c. performance of a task carried out in the public interest or in the

		exemption for organizations with fewer than 250 employees. **Article 34** It is impractical for data controllers to produce potentially lengthy records on the request of a data subject, and may require the exposure of corporate confidential information such as security practices. It also does not seem to serve any particular data protection objective as this right can be addressed through one of the other rights of data subjects (e.g., right to access and correct). **Article 36.1** The time frame provided for correction of personal data is impractical and out of step with international practice. **Article 38** It is unclear how the "approval" here relates to the broader framework under which personal data can be processed under the various alternative bases for data processing in Article 20. This should be clarified. **Article 39** The lack of clarity on retention and requirements for deletion make it impossible to fulfil this directive. **Article 40.1** The obligation to erase personal data should be subject to a condition that retention is no longer necessary for legal or business purposes. **Article 40.3** This provision is confusing. It contemplates that personal data that is deleted should be recoverable,	exercise of official authority vested in the controller, including on the grounds of public interest in the area of public health; d. archiving purposes in the public interest; e. scientific or historical research purposes or statistical purposes; or f. the establishment, exercise or defense of legal claim. **Article 38** We recommend amending the Bill to clarify how the "approval" under Article 38 relates to the broader framework under which personal data can be processed under the various alternative bases for personal data processing in Article 20. **Article 40.1** We recommend amending Article 40.1 to read as follows: "Personal Data Controllers must delete Personal Data in its possession or under its control in the event that the Personal Data is no longer needed to achieve the purpose for which it was collected or otherwise processed, and retention is no longer necessary for legal or business purposes." **Article 40.3** We recommend deleting Article 40.3 in its entirety. **Article 41** We recommend clarifying the difference between "destruction" of personal data under this Article and "deletion" of personal data under Article 40. To

		which suggests that the data is still being stored somewhere (and is not fully "deleted"). It is therefore unclear what the data controller's obligation under this provision is, and this should be clarified. **Article 41** It is unclear how "destruction" of personal data under this Article differs from "deletion" of personal data under Article 40. To the extent that they mean the same thing, Articles 40 and 41 should be merged and streamlined. **Article 42** When developing data breach notification provisions, it is critical to recognize that not all data breaches represent equal threats. In many instances, data breaches pose no actual risks to the individuals whose data was compromised. To ensure that consumers are not inundated with notices regarding immaterial data breaches, the notification obligation should be triggered only in circumstances where the breach results in a material risk of harm. For instance, the obligation to provide notice should not apply to instances in which the breached data is unusable, unreadable or indecipherable to an unauthorized third party through practices or methods (e.g., encryption) that are widely accepted as effective industry practices or industry standards. Finally, it is critical that data controllers are afforded adequate time to perform a thorough risk assessment to determine the scope of the security risk and prevent further disclosures. It is therefore counterproductive to include within the data breach provision a fixed deadline for providing notification.	the extent that they mean the same thing, we recommend merging and streamlining Articles 40 and 41. **Article 42** We recommend revising Article 42, in line with our comments in the previous column, to be consistent with international practices on data breach notification. **Article 43** We recommend amending Article 43 to read as follows: "The Data Processor and any person acting under the authority of the Data Controller or of the Data Processor, who has access to personal data, shall not process those data except on instructions from the Data Controller, unless required to do so by a law of Indonesia." **Article 44.4** We recommend deleting Article 44.4 in its entirety. **Article 45** We recommend deleting Article 45 in its entirety. **Articles 46, 47** We recommend amending Articles 46 and 47 to keep the duties general, and deleting Article 47.3 in its entirety. **Articles 48, 68 – 77** We recommend amending Article 48 to include a graduated process (e.g., warnings to mediation to penalties), and deleting Articles 68 – 77 in their entirety. Additionally, we recommend including in

		Accordingly, instead of the fixed 72 hours contemplated by this Article, the notification should be subject to a "no undue delay" requirement. There should also be a two-step process for processors to notify controllers before they notify authorities/individuals with separate timelines. The timeline for notification should only begin once the controller (ideally the DPO) is aware of a significant breach. All access to information and facilities under the Law should be subject to checks and balances and judicial oversight to ensure that rights of individuals and private actors are protected and that the potential for abuse of power is limited. Any access to information or facilities should be required with a valid court order. There should also be rights for data controller to dispute or contest the order, command, or request. Orders, commands or requests should be limited to situations where there is a significant risk of serious harm, and such harm should be balanced against other criteria, such as impact on the community, commercial and other practical impacts. The Bill should include clearer obligations on the relevant regulator to maintain the confidentiality of information provided to them and to protect the information from unauthorized disclosure / use and to securely dispose of the information after their investigation is completed or the information is no longer required by the regulator for its legitimate supervisory purposes. **Article 43**	the Bill a clear framework for due process and the right of appeal against administrative decisions.

		This requirement is highly problematic as it blurs the obligations of data controllers and data processors without regard for their respective roles in the data lifecycle and differing visibility and degree of control over the decisions for collecting and processing personal data. It also conflicts with Article 44 which appears to place the primary obligation for compliance with the Bill on the data controller. This provision is in complete contrast to modern data protection laws that make a very clear distinction between the roles of data controllers versus data processors (e.g., the GDPR and the Philippines Privacy Law). In line with international practice, the data processor should only have the obligation to comply with the lawful instructions of the data controller. **Article 44.4** Under Articles 44.1, 44.2 and 44.3, it is fairly clear that as long as a data processor processes personal data in accordance with the purposes specified by the data controller, then the data controller remains the one responsible for the processing of the personal data. However, as with the comments on Article 43, Article 44.4 imposes impractical obligations on the data processor. The data processor should only be responsible for complying with the lawful instructions of the data controller and be responsible for the harm suffered by the data subject if they act outside of such instructions. A data processor cannot have the same responsibilities as a data controller as this would be impractical, and in some cases potentially impossible to implement. **Article 45**	

		The introduction of a third party in this provision creates uncertainty in the data processing chain and should be removed. **Articles 46, 47** Articles 46 and 47 require the appointment of a data protection officer (DPO) for public services, systematic large-scale monitoring of data or processing data relating to criminal action. We propose deleting the provision whereby additional requirements/provisions can be introduced by ministerial regulations and to keep the duties of DPOs general. **Articles 48, 68 – 77** Article 48 sets out sanctions that include suspension of activity, deletion of data, compensation or a fine. Articles 68 – 77 set out additional criminal penalties for specific infringements that max out at $7m. While a central regulator should have the tools and resources necessary to ensure effective enforcement of privacy laws, remedies and penalties should be proportionate to the harm resulting from violations of data protection laws. Criminal penalties are not proportionate remedies for violation of data protection laws, would be inconsistent with internationally-recognized best practice, and are likely to chill legitimate data processing activities. We therefore recommend the removal of all criminal provisions from the Bill. Additionally, with respect to civil or administrative penalties, there should be a graduated process (e.g., from warning to mediation to penalties). A clear framework for due process and the right of appeal against administrative decisions should also be included in the Bill.	

VII on Personal Data Transfer and Diversion	49 - 52	The free flow of data across borders confers multiple benefits for economies and the financial services ecosystem. Open markets, and the ability to move data relatively freely across national borders, have helped facilitate a number of innovative developments over the past decade. These advances include cloud computing and ongoing progress with Smart Cities and the Internet of Things (IoT). Such developments have conferred significant economic benefits, including productivity gains, lowered costs for consumers, and increased employment. As electronic commerce continues to grow and digital technologies become ubiquitous, the ability of organizations to easily share data across borders is essential. Free cross-border data flows also enable entrepreneurs in developing regions to take advantage of the data infrastructure outside their home countries. This helps bring new and/or enhanced services to local consumers and businesses. Additionally, we would like to reiterate the importance of cross-border data flows to economic growth and development. Rapid advances in technology have changed the way business is conducted around the world. As ITIF notes, global digital trade is increasing rapidly and thus spurring economic growth, driven by increasing usage of cloud-based internet services. With digital trade and cross-border data flows expected to grow faster than the overall rate of global trade, any impediments to data movement can have profound consequences for economies. To optimize data transfers on a global scale and ensure smooth cross-border data transfers in a	**Articles 49-51** We recommend that a possible provision that could be used in place of Articles 49 to 51 could read as follows: "The Personal Data Controller is responsible for any personal data under its control or custody, including information that have been outsourced or transferred to a Personal Data Processor or a third party for processing, whether domestically or internationally. A Personal Data Controller may transfer Personal Data outside the jurisdiction of the Republic of Indonesia if: (a) it is satisfied that the country to which the Personal Data will be transferred provides an comparable or higher level of personal data protection as this Law; (b) there is a contract between the Personal Data Controller and the recipient of the personal data; (c) there is an international agreement between the countries; (d) the Data Subject has consented to the transfer; (e) the Data Controller has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available; (f) there are applicable binding corporate rules regarding personal data protection between members of a corporate group (g) the transfer is necessary for the performance of a contract between the data

		global manner, thereby maximizing the benefits of cloud and Internet-based services, it is vital that efforts be made through a broader multilateral approach, such as participation by Indonesia in developing multilateral frameworks such as the APEC Privacy Principles and the Cross-Border Privacy Rules system. **Articles 49-51** The current drafting of the data transfer regime is unusually complicated with provisions for (a) general transfers of personal data to other parties under Article 53, (b) transfers within Indonesia and (c) transfers outside of Indonesia. It is unclear for example why there should be separate provisions for transfers to third parties generally at all. Additionally, the list of permitted transfer mechanisms under Article 51 (for transfers of personal data outside of Indonesia) is much more restrictive than those in other countries' laws, which tend to also include binding corporate rules and approved certification mechanisms. Instead of restricting the permissible scenarios for international transfers to just the 3 mechanisms listed in Article 51, we would suggest that the framework for international transfers should simplified and be based on the OECD principle of "Accountability". This principle requires the data controller to remain responsible for the transfer of personal data to third parties whether within Indonesia or outside of Indonesia. This is because the data controller typically is the party that knows the purposes for which the personal data has been collected and has the direct relationship with the	subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (h) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; (i) the transfer is necessary for important reasons of public interest; (j) the transfer is necessary for the establishment, exercise or defense of legal claims; the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent." **Article 52.1** We recommend deleting Article 52.1 in its entirety.

		data subject to provide relevant notifications / obtain relevant consents from them. Under such an "Accountability" approach, the 3 mechanisms in this Article can be listed as non-exhaustive examples (along with the other examples above, e.g. binding corporate rules and approved certification mechanisms) where an organization would be deemed to have met the accountability principle. This would bring the regulation in line with GDPR as well as other regional privacy laws such as in the Philippines, Singapore, and Malaysia. Additionally, the multilateral frameworks (such as the APEC Privacy Principles and the Cross-Border Privacy Rules system we mentioned above) could be listed (perhaps in implementing regulations) as an example of an international agreement and/or certification mechanism, which would provide further clarity to the industry on how they can validly transfer Personal Data outside of Indonesia. Notwithstanding the above, we would also appreciate clarification on: (1) how the requirement of "personal data protection level that is equal to or higher than this law" under Article 51.a.; and (2) what would be sufficient to satisfy the "international agreement" requirement under Article 51.c. **Article 52.1** In the event of an acquisition, merger etc. it may be impractical to notify all data owners of the transfer of data. This requirement should be deleted.	
VIII	53 - 60	**Article 56**	**Articles 56, 57, 59**

on Prohibition in Personal Data Use		This provision appears to repeat Article 45 and should be deleted. **Article 57** This provision appears to repeat Articles 50 and 51 and should be deleted. Please see our comments on Articles 49 - 51 above instead. **Articles 58, 59** Article 58 requires consent for processing for commercial purposes and for profiling and Article 59 requires consent for processing data that is not an entity's property. It is unclear how these Articles relate to Articles 20, 22 and 25, among others. There is no need for these additional Articles 58 and 59, as they appear to simply cover specific *examples* of when data can be processed with consent. They should be deleted to avoid confusion. In any event, this obligation should only apply to data controllers. Data processors typically have no visibility into the purposes for which the personal data has been collected or the scope of the consents provided. Moreover, data processors do not typically have direct relationships with data subjects to be able to practically obtain consents. What constitutes "commercial purposes" under Article 58 is also far too broad and it is unclear what this is intended to protect. A clear definition of profiling should also be included.	We recommend deleting Articles 56, 57 and 59 in their entirety. **Article 58** We recommend deleting Article 58 in its entirety and including a definition for "profiling".
IX on Establishment of Personal Data Control	61	The purpose of this provision (and the conduct guidelines it contemplates) is unclear.	We would appreciate clarification on the purpose of this provision (and the content guidelines it contemplates).

Conduct Guideline			
X on Exceptions in Personal Data Protection	62	**Article 62** The exemptions should be expanded to include: (a) anonymized data and pseudonymized data, (b) data processed for historical purposes, (c) Personal data processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations, (d) processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity We also propose that employee data or categories of employee data should be exempted and included here. **Article 62 point c** Does this include the *Sistem Layanan Informasi Kredit* reporting to OJK? **Article 62 point e** Must take into account measurement and measurement analysis. The way this is phrased, it only allows for the processing of aggregate data. However, much individual data is processed for aggregate reports.	**Article 62 point e** It is necessary for aggregate data in which the processing is done for statistical, *measurement, measurement analysis,* and scientific research interests.
XI on Dispute Settlement	63		
XII	64		

on International Collaboration			
XIII on Roles of Government and Society	65 - 67	On data protection authority, an independent enforcement body should be established. The Bill hints that this will be shared between sectoral regulators and the appropriate ministry, which is not ideal.	
XIV on Criminal Provisions	68 -77	We reiterate that criminal penalties are not proportionate remedies for violation of data protection laws and we therefore recommend the removal of all criminal provisions from the Bill. (See also our comments to Article 48 above.)	We again recommend deleting Articles 68 to 77 in their entirety.
XV on Transitional Provisions	78	We appreciate the government's efforts to protect personal data in order to ensure the security and personal protection of the public, and we are committed to supporting these efforts. In its implementation, there are potential obstacles especially for industries that collect and process a lot of customer data (e.g., the financial services industry) Therefore, we strongly recommend that parties be allowed at least **two (2) years** to comply with the provisions of the Bill. We further recommend that personal data that have been collected and/or processed by data controllers and/or data processors (under and in compliance with existing applicable regulations) should be excluded from the scope of the Bill.	We recommend amending Article 78 to provide at least two (2) years (after the Bill comes into force) for parties that collect and process personal data to comply with the law. We further recommend including a provision to exclude personal data that have been collected and/or processed by under existing applicable regulations from the scope of the law.
XVI on Closing Provision	79 - 80		