ASIA
INTERNET
COALITION

07 April 2020

To
Mr Johnny G. Plate
Minister of Communications and Information Technology
Ministry of Communications and Information Technology (KOMINFO)
Jl. Medan Merdeka Barat no. 9, Jakarta 10110 Indonesia

Ms. Meutya Hafid
Chairperson of Commission I
House of Representatives of the Republic of Indonesia

Mr. Semuel A. Pangerapan
Director General of Application Informatics
Ministry of Communication and Informatics

Subject: AIC Submission on Indonesia's Draft Indonesia Personal Data Protection Law

Dear Minister Plate,

The Asia Internet Coalition (AIC) and its members express our sincere gratitude to the Ministry of Communications and Information Technology (KOMINFO) and the Government of Indonesia for the opportunity to submit comments on the **Indonesia's Draft Personal Data Protection Law.**

The AIC is an industry association comprised of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our member companies would like to assure KOMINFO that they will continue to actively contribute to the security of digital platforms, products and services in support of the digital economy goals of Indonesia. Our members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, Grab, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media), and Booking.com. In these unprecedented times we also commend Indonesia's strategy in fighting the COVID-19 pandemic and express our solidarity in the government's efforts, to which technology has been playing a critical role.

In the backdrop of digitalization and growth of digital services across the world, the role of data has become more and more significant. This has given rise to concerns of informational privacy and the exercise of rights over personal data. Without a framework to govern these two subjects, no digital industry can be sustainable. In this context, the Personal Data Protection Law is a much-needed effort and parallels the global movement towards data protection legislations.

Although we appreciate the Government of Indonesia and KOMINFO's efforts towards developing the **Personal Data Protection Law**, we believe that there are concerns regarding its provisions, and suggest that they be aligned with global best practices.

In this regard, we are grateful to be able to present our recommendations, and would also like to re-state our continuous support and assistance to the Government in its efforts to bring about this transformational change in the privacy landscape in Indonesia.

As such, please find appended to this letter detailed comments and recommendations, which we would like KOMINFO to consider. Section A of this submission provides our feedback on key issues and recommend general approaches to formulating an operationally practicable Personal Data Protection regulatory framework in line with global best practices. Section B provides recommendations with specific line changes to the Draft Law.

We are grateful to KOMINFO for upholding a transparent, multi-stakeholder approach in developing this regulation. Furthermore, we welcome the opportunity to offer our inputs and insights on industry best practices, directly through meetings and discussions and help shape the dialogue for the advancement of the digital ecosystem in Indonesia.

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

Sincerely,

Paine

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

SECTION A

Recommendations on General Approaches to the Draft Law

1. **Further enhancements for cross border data flows framework (Article 49):** The free movement of data underpins the digital economy and plays a fundamental role in ensuring data-driven growth and innovation. The effective and efficient functioning of data processing across borders is a fundamental building block in any data value chain. Therefore, we support Indonesia's introduction of a cross-border data flow framework that explicitly permits the transfer of data overseas, provided that the regulated entity takes reasonable steps to ensure that personal data transferred overseas continues to be protected at a comparable standard to that of Indonesia's data protection legislation. To further enhance the framework, we recommend that in addition to the mechanisms for cross-border data transfers in Article 49 (b, c, d), the law should explicitly include the following non-exhaustive list of measures that an entity can take to demonstrate that it has taken such reasonable steps such as:

    a. the Personal Data Controller assessing that the overseas data recipient is bound by comparable obligations under their applicable laws;
    b. ensuring the recipient is bound by binding corporate rules; or
    c. verifying that the recipient has established systems and processes that comply to internationally recognized standards such as requisite ISO certifications.

    We recommend expanding the number of legal bases which allow international transfer that is more aligned with international norms and harmonised with global data governance frameworks. If there are no international agreements in place between Indonesia and the non-Indonesia jurisdiction receiving the data, adherence to internationally recognized security standards should suffice. The Bill should clarify that consent is one basis for transfer but is not required for all transfers, in line with the APEC Cross Border Privacy Rules Framework and OECD Privacy Principles.

2. **Response time to user requests.** We would like to recommend the government to provide a reasonable and adequate time for companies to verify and respond to such requests. This is especially true under circumstances where data controllers and/or processors may need more time to process such requests or to keep processing for legitimate business interest or continuity of services (e.g. processing outstanding payment, fulfillment of services, delivery, etc.)

3. **Additional clarity between the responsibilities of the Personal Data Controller and the Personal Data Processor (Articles 43 and 44)**. We support Indonesia's approach of demarcating between the responsibilities of Personal Data Controllers and Personal Data Processors, as outlined in Article 43 of the Draft Law. However, Article 44 is confusing as it makes references to obligations that should be placed on Personal Data Controllers and not

Personal Data Processors. Specifically the following obligations ought to rest with the Personal Data Controller and *not* the Personal Data Processor: (i) Article 27 on the Personal Data Controller protecting and ensuring the security of the personal data; (ii) Article 28 on Personal Data Controller supervising the Personal Data Processor; (iii) Article 29 on the Personal Data Controller ensuring that the protection of data from invalid processing; (iv) Article 30 on Personal Data Controller preventing illegal access; (v) Article 31 on Personal Data Controllers maintaining a record; and (vi) Article 35 on Personal Data Controllers guaranteeing the accuracy, completeness, and consistency of the personal data. Therefore, we recommend a clear guideline and demarcation on the roles and responsibilities of Data Processor and Data Controller. There are instances where a Data Processor may process data for different purposes than those of Data Controller. We'd like to seek clarifications on what institutions are considered data processors, controllers, data subject, and third-party.

Personal Data Processors often do not have sight of their customer's data and will not be able to establish whether personal data is being processed, and therefore cannot reasonably be expected to know when and whether they should put in place processes to comply with PDP obligations. Instead, Personal Data Processors should be expected to implement reasonable and appropriate security measures for their Electronic System. We therefore recommend that Article 44 be deleted in its entirety. Instead, the Government of Indonesia can consider amending Article 43 to include similar language in Article 21(1) on confidentiality, and the responsibilities of a Personal Data Processor to implement reasonable technical and organizational standards at the instruction of the Personal Data Controller.

4. **Creation of a notifiable data breach framework (Article 40).** We recommend that notifiable data breach notification frameworks should clearly identify the unauthorized disclosure of, or access to personal data which may cause a material risk of identity theft or economic loss to data subjects. Therefore, a clearer definition for the events that will trigger "data breach" should be provided. Further, a materiality threshold is necessary for the framework to ensure that notifications made to regulators or data subjects are of breaches that require the greatest attention and expedient mitigation. The trigger for legal requirement to notify regulators or users of a data breach should be based on a materiality threshold that looks at the impact of the breach on the affected data subjects, such as introducing a clear threshold for breach notifications based on level of "harms" and identifying specific types of data that inherently pose a risk to users if subject to breach. Without such a threshold, numerous immaterial notices will be issued resulting in "notification fatigue" which would in turn lead to inconvenience for Data Subjects, increase in administrative costs and burdens for the regulator, and result in Data Subjects and regulators failing to take appropriate action in response to notifications that indicate a real risk of harm.

   Data breach notification requirements in the Draft Law should clearly specify that Personal Data Controllers are responsible for managing data breach notifications. It would not be appropriate for Personal Data Processors to be responsible for data breaches, including notification obligations, as Personal Data Processors do not have visibility of Personal Data Controllers' content. This means that Personal Data Processors are not able to distinguish security breach incidents that disclosure or modify personal data, from incidents that do not cause adverse material impact on personal data. Finally, Personal Data Processors do not have direct relationships with the data subject and would therefore not be able to meaningfully or effectively communicate matters relating to a personal data breach with them.

   In addition, if data breach notification frameworks are introduced, we recommend that authorities provide guidelines around when a data controller becomes "aware" of a breach and has to report it. Personal Data Controllers should be provided a reasonable window of time to investigate and confirm a breach before requiring notification to regulators or Data Subjects.

5. **Clarifying provisions to avoid joint and several liability, removal of individual liability and criminal penalties, and incorporating due process and appeals mechanisms (Article 13, Article 51, and Chapter XIII).** We recognize and understand the Indonesian government's desire to ensure sufficient enforcement powers for the Data Protection Authority (DPA) to be effective. To this end, we propose the following clarifications and revisions to improve the overall enforcement framework.

   a. **Delete Article 13 which provides a right of private action.** The DPA should be the sole enforcer of data protection laws as it is best positioned to ensure consistent and clear compliance by all organizations. A parallel private right of action will lead to burdensome administration of enforcement under the laws, with no practical limits on the numbers or frequency of complainants. Further, possible inconsistencies in interpreting this Article will allow adjudicating officers of private actions wide discretionary powers, leading to uncertainty among businesses in Indonesia. Therefore, we recommend that Article 13 be deleted in its entirety.

   b. **Remove Article 51 and 61, to ensure that employees cannot be made individually liable for the offences of the body corporate and remove criminal penalties under Chapter XIII as such criminal penalties are disproportionate to the Draft Law.** This law should be clearly applicable to organizations and corporations rather than individuals. This Draft Law has removed the concept of Individuals providing data on behalf of third parties in comparison to the previous versions; Article 51 now outright prohibits the processing of personal data by an individual, on behalf of a third-party, potentially even for when a the individual is acting in his personal or domestic capacity. When read together with Article 61 on penalty provisions, it imposes significant and severe penalties (including imprisonment), even where individuals are (a) acting in personal or domestic capacity, or (b) employees acting at the behest of their organizations. Imposing direct liability on an individual is disproportionate as data protection legislations are intended to govern the actions of a body corporate or an organization, rather than an employee or an individual in their private capacity. We therefore recommend that Articles 51 and 61 be removed from the Draft Law. Similarly, given that individual liability should be excluded from data protection laws, the criminal penalties in Chapter XIII are not proportionate remedies for the violation of data protection laws as these penalties address individual employees. Therefore, criminal penalties should not be included in privacy frameworks, and we recommend the removal of all criminal penalties from the law.

   c. **Include clear and defined due process and appeals mechanisms.** Separately, the Draft Law should clearly define due process mechanisms allowing organizations to appeal decisions and outline specific remedies and penalties. The law should not impose strict liability. Instead, organizations should be able to demonstrate that they have taken appropriate security and organizational measures to protect personal data in the circumstances. For example, both under the EU General Data Protection Regulations

(**GDPR**) (Article 83) and the Singapore Personal Data Protection Act 2012 (Section 29), penalties are meted out "depending on the circumstances of each individual case". The GDPR for example, takes into account the "nature, gravity and duration of the infringement", whether the breach was due to "intentional or negligent character" of the data controller or processor, and whether any action was taken to mitigate the damage suffered by data subjects amongst other factors.

6. **Territorial applicability of the law to be reasonably scoped (Article 2)**. The territorial reach of PDP regulations should be clearly demarcated to ensure clarity for businesses looking to comply with the framework, and enable the DPA to enforce regulations effectively. We recommend limiting the application of the data protection law to data processing performed by an individual or legal entity, whether public or private, provided that: (1) the scope of the legislation extends only to residents who are within Indonesia at the time their personal data is processed (including collected, used or disclosed); and (2) the individual or entity processing the personal data is established in Indonesia. We suggest that the legislation target "residents" of Indonesia rather than "citizens" to ensure that all residents are treated equally but also to ensure that non-resident citizens of Indonesia are not unintentionally covered by conflicting laws. Data Protection regimes that maintain extra-territorial reach face challenges with enforceability, and result in dissatisfied complainants and citizens who have the expectation that their data protection concerns can be addressed regardless of where the processing activity has occurred. This places immense pressure on the resources of the DPA and could result in the perception that the DPA is ineffective. In addition to enforceability challenges, extra-territorial privacy laws can create conflicting and overlapping data protection obligations that make compliance both overly complicated and costly for companies, including Indonesian SMEs that have a multi-country presence. This ultimately detracts from the aim of privacy laws to protect personal data.

7. **Create a simple and clear framework to ensure ease of compliance for organizations implementing the Draft Law.** Data Protection Laws should avoid imposing requirements that generate disproportionate administrative burdens on organizations, without providing additional protections for the data subject. In addition, concepts and definitions in the legislation must be clear and reasonably scoped, otherwise there will be significant uncertainty amongst organizations when implementing data protection compliance programs. Such requirements include the following:

    a. **The requirement to delay or limit personal data processing in Articles 12 and 26 are a duplicate of Articles 8 and 9, and can be confusing for organizations to implement.** Chapter III already affords the right for data subjects to request for the processing activity to be terminated (Article 8), and to withdraw consent (Article 9). While laws such as the GDPR also include similar rights – including the Right to Object (Article 21) and the Right to Restriction of Processing (Article 18) – these rights are clearly limited to specific purposes (e.g. direct marketing, lawful basis for processing and automated decision-making). However, the Draft Law does not associate any similar activities or purposes to Article 12. Furthermore, the Draft Law already includes the Right to Object Automated Decisions under Article 10. We therefore recommend that Articles 12 and 26 be deleted for clarity and to avoid duplicative and confusing obligations on organizations.

    b. **Avoid requirements that create undue burdens on organizations to retain a record of activities (Article 31) of processing**. Article 31 currently requires Personal Data

Controllers to record *all* activities. Such a requirement is impractical because it creates a disproportionate administrative burden for regulated entities, and does not offer an additional level of protection to personal information. It would also divert DPA resources from the investigation and enforcement of serious data breaches, if the DPA has to ensure that organizations are compliant. We therefore recommend that Article 31 be deleted.

c. **Expand the grounds for processing of personal data and incorporate concepts of deemed or implied consent (Articles 18, 19, 20, 24).** We support the Draft Law's inclusion of additional bases for processing other than consent, under Article 18(2). However, the relief it offers from the rigors of consent based processing under the Bill is limited because it does not include contractual necessity or legitimate business interests, both of which are essential grounds for the smooth functioning of businesses. These additional legal bases are also necessary to ensure that developments in technology, particularly IoT, are supported by the lawful collection of personal information. We also note that such legal bases are exceptions to the consent requirement. All legal bases set out in the legislation for collecting, using and disclosing personal data should be treated equally instead of relying on consent as the primary ground for processing personal data. Overly stringent requirements for consent will slow the provision of goods and services to consumers and increase compliance costs without necessarily increasing security for data subjects. We therefore recommend that the Draft Law be expanded to include (but not limited to) the following bases for processing: (i) prevention and detection of any unlawful activity including fraud; (ii) collection where necessary for evaluative purposes; and (iii) processing where necessary for the purposes of the legitimate interests pursued by the Personal Data Controller, Personal Data Processor, or a third party.

In addition, Articles 19 and 20 should also be amended to allow for both express and implied consent. 'Written' or 'verbally recorded' consent may not be always practicable and such a requirement would significantly affect the ease of doing business. For example, when a Data Subject hands over a credit card to a retailer to process a payment, their consent for the collection, use and disclosure of their personal data (i.e. credit card payment data) for the purposes of processing the payment can be implied through their actions. It would be significantly onerous for retailers to have to notify, explain, and record explicit consent for every payment process. Such a requirement would significantly impede the ease of doing business, and does not add additional protection for the data subject. The Singapore Personal Data Protection Act (2012), includes deemed consent bases under Section 15, in which a data subject's consent can be "deemed" if the data subject voluntarily provides the data for a purpose and it is reasonable that the data subject would do so. We therefore recommend that Article 19 and 20 be amended to include the concept of deemed and implied consent. Doing so would ensure that the Data Subject's rights remain protected, without significantly impeding the ease or speed of doing business.

Article 24 also requires Personal Data Controllers to provide a specified list of information to data subjects prior to obtaining consent. These requirements should avoid over-prescribing, and must also address circumstances where consent can be deemed (as shown in the example previously on payment processing), or where an organization carries out the processing by relying on a bases other than consent. In this regard, we propose amendments to streamline Article 24(1) (as reflected in Annex A). We also recommend that Article 24(2) be deleted as the requirement to obtain "consent evidence" prior to data collection is onerous and impracticable if data controllers rely on deemed consent or bases other than consent.

d. **Ensure that reasonable timeframes for such activities are included (Art. 24, 25, 34)**. Articles 24, 25, and 34 prescribe that organizations must accede to a data subject's request to access information on consent and processing activity (Art. 24) in 7 days, cease processing following the withdrawal of consent (Art 25.) in 3 days, and correct errors or update the data (Art. 34) in 1 day. These timeframes are extremely tight and in some cases simply would not be practicable. For example, organizations may have existing timelines for verifying a requestors identity, accounting cycles, and closing of accounts (e.g. 14 or 21 days), and consolidating all the information requested would also take time (e.g. if the requestor asks for a significant amount of information contained in multiple sources). We therefore recommend that the Draft Law avoid being over-prescriptive and remove the specific timeframes. Instead, we recommend incorporating language similar to "as soon as reasonably practicable" as it places the accountability on the organization to demonstrate that it has acted reasonably given the nature of the activity.

e. **Avoid the inclusion of anonymized and pseudonymized data from the scope of the Draft Law (Article 11).** The Draft Law does not define "pseudonymized data", however it includes requirements on the treatment of pseudonymized data in Article 11. We recommend that anonymized or pseudonymized personal data should not be defined as "personal data", and should be clearly excluded from data protection legislation. This is the case as anonymized or pseudonymized data is already de-identified and no longer pertains to specific individuals (e.g. if the data is aggregated, or noise is introduced into the dataset). Excluding such data will ensure that organizations correctly understand what constitutes personal data, so that they focus their resources on protecting and creating appropriate governance processes for personal data. Furthermore, the right for data subjects to object or approve 'pseudonymization' will create an undue burden for organizations to create separate processes for using non-personal data. Such a requirement will impede an organization's legitimate business activities whilst not adding any additional protection for the Data Subject. This approach is recognized by regional frameworks such as the OECD Privacy Principles, the privacy laws of other countries (e.g. Singapore, New Zealand, Australia) and under the EU's GDPR, which is often seen as a high benchmark for privacy laws.We therefore recommend that Article 11 be deleted.

SECTION B

List of Specific Issues and Recommendations

1. Chapter I, Article 1: Definitions

In this Law, the definition of:

1. *Personal Data is any data about a person that is identified and/or could be identified individually or combined with other information either directly or indirectly through electronic and/or non-electronic system*
2. *Information is explanations, statements, ideas, and signs that contain values, meanings, and messages, both data, facts, or elucidation that could be seen, heard, and read which are presented in various formats in accordance with the development of electronic or non-electronic information and communication technology.*
3. *Personal Data Controller is the party that determines the purposes and has the control of processing personal data.*
4. *Personal Data Processor is the party that processes personal data on behalf of the personal data controller.*
5. *Personal Data Subject is an individual person as the data subject who owns the personal data attached to them.*
6. *Individuals are individual person or Corporation.*
7. *Corporation is number of organized persons and/or assets, both legal entities and non-legal entities in accordance with provisions of the legislation.*
8. *Public Authority is the executive, legislative, judiciary, and other agencies with main function and task related to the state administration, of which part or all of the funds sourced from the State Revenue and Expenditure Budget and/or Regional Revenue and Expenditure Budget, or non-governmental organization in so far as part or all the funds sourced from the State Revenue and Expenditure Budget and/or Regional Revenue and Expenditure Budget, the society and/or international contribution.*
9. *Minister is the minister who organizes government affairs in the field of communication and information technology.*

Recommendation:

Article 1(1): The definition of “Personal Data” should expressly exclude anonymized, de-identified and/or pseudonymized data subject to restrictions on re-identification, such as those outlined in Recitals 26, 28 and 29 GDPR. This approach is recognized by regional frameworks such as the OECD Privacy Principles, the privacy laws of other countries (e.g. Singapore, New Zealand, Australia) and under the EU's GDPR, which is often seen as a high benchmark for privacy laws

Furthermore, “person” is defined in Article 1(6) as including both individual persons and corporations. The definition of “Personal Data” is consequently broader than under International Benchmarks such as GDPR, Singapore’s PDPA, Hong Kong’s PDPO and Japan’s APPI. To include corporate data in the definition of “Personal Data” may also blur the line with other laws such as trade secrets and confidential information which typically protect business data. Legal entities should not have the same rights in personal data as individuals and different laws should protect business data. The definition of “Personal Data” should therefore be limited to natural persons.

In this Law, we suggest the following for the definition of Personal Data:

Personal Data is any data reasonably linkable to an identifiable natural person or to a device associated with an identifiable natural person. Personal data does not include data which is:

- anonymized
- aggregated
- pseudonymized
- employee data
- public information
- generated

Article 1(4): Definition of Data Processor only refers to a party that does data processing on behalf of Data Controller. This does not adequately address instances where a Data Processor may process data without specific instructions from a Data Controller, but instead from a Data Owner. There needs to be a clear guideline and demarcation on the roles and responsibilities of Data Processor and Data Controller. There are instances where a Data Processor may process data for different purposes than those of Data Controller. We also seek clarity on what institutions the government considers to be processors, controllers, data subject, and third-party.

Article 1(5): Definition of “Personal Data Subject” (Art. 1(5))

We understand that a more accurate translation of this term is “Personal Data Owner” or “Owner of Personal Data”. The concept of “ownership” should be removed from this definition as it is not appropriate. Replacing “owner” with “subject” is more aligned with international best practice.

We suggest amending Article 1(5) to the following:

- Personal Data Subject shall be a natural person to whom as Personal Data relates.

2. Chapter I, Article 2: Extraterritorial Application of the Law

"This Law applies to Individuals, Public Authority, and organization/institution that carries out legal action as regulated in this Law, both within and outside the jurisdiction of the Republic of Indonesia, which has legal consequences within the country's jurisdiction and/or for Indonesian personal data subject outside the jurisdiction of the Republic of Indonesia."

Recommendation: The Bill envisages applicability to Indonesian citizens worldwide. This raises a conflict of laws issue. For example, if an Indonesian citizen lives in (or travels to) the EU, they will be under the Indonesian PDPB. However, the GDPR is also likely to apply to the processing of the personal data of that Indonesian citizen. In order to align with international law on extraterritoriality, GDPR limits its territorial scope to "data subjects who are in the Union" (rather than EU citizens, regardless of their location). Even with extraterritoriality aside, compliance with the Indonesian PDPB would raise practical issues. It would require verification of the citizenship of every data subject globally in order to identify if they are Indonesian and therefore apply the provisions to the processing of their data. It is more practical and reliable to process personal data based on the data subject's location. The scope of the Indonesian PDPB should be consistent with international benchmarks, such as the and be aligned with GDPR, to avoid these legal and practical issues.

We therefore, recommend that:

- This Law applies to the processing of Personal Data in the context of the activities of an establishment of a Personal Data Controller or a Personal Data Processor in the Republic of Indonesia, regardless of whether the processing takes place in the Republic of Indonesia or not.
- this Law applies to the processing of Personal Data of Personal Data Subjects who are in the Republic of Indonesia bya Personal Data Controller or a Personal Data Processor not established in the Republic of Indonesia, where the processing activities are related to: (i) the offering of goods or services, irrespective of whether a payment of the Personal Data Subject is required, to such Personal Data Subjects in the Republic of Indonesia; or (ii) the monitoring of their behaviour as far as their behaviour takes place within the Republic of Indonesia

We suggest amending Article 2 to the following:

1. This Law applies to:
   a. any Person who processes; and
   b. any Person who has control over or authorizes the processing of any personal data in respect of commercial transactions.

2. Subject to subsection (1), this Law applies to a Person in respect of personal data if: the Person is established in the Republic of Indonesia and the personal data is processed, whether or not in the context of that establishment, by that Person or any other Person employed or engaged by that establishment;

3. This Law shall not apply to any personal data processed outside the Republic of Indonesia.

3. Chapter II, Article 3: This Article specifies definitions of Personal Data, differentiates between Specific Personal Data and General Personal Data, and further defines what falls under Specific Personal Data

(1) Personal Data consists of:
- a. General Personal Data; and
- b. Specific Personal Data.

(2) General Personal Data as referred to in paragraph (1) letter a includes:
- a. full name;
- b. sex;
- c. citizenship;
- d. religion; and/or
- e. Personal Data that is combined to identify a person.

(3) Specific Personal Data as referred to in paragraph (1) letter b includes:
- a. health data and information;
- b. biometric data;
- c. genetic data;
- d. sexual life/orientation;
- e. political view;
- f. criminal records;
- g. child data;
- h. personal financial data; and/or
- i. other data in accordance with the provisions of the legislation.

Recommendation: The definition of "Personal Data" in the Bill is not sufficiently clear. Further, throughout the law references to these different classifications of data is no longer used. The Law should clearly refer to which Personal Data is applicable and clarify what is the intention to impose separate or stricter rules for Specific Personal Data.

In the first instance, the definition of "General Personal Data" should be removed as the Bill does not differentiate between the treatment of General Personal Data and other types of Personal Data. Hence, having a reference to "General Personal Data" is unnecessary. We instead recommend a clarification of the definition of "Personal Data" (see Comments in Article 1) .

The Bill should provide an exhaustive, closed list defining the scope of "Specific Personal Data" and should not include an umbrella term such as, "other data in accordance with the laws and regulations" so as to ensure that data owners can understand and enforce their rights and businesses can have certainty and be able to better manage their costs of compliance.

"Specific Personal Data" should be an exhaustive list without reference to other laws and should clearly be a subset of "Personal Data".

As not all personal financial data is sensitive, this should not be included within the category of Specific Personal Data.

Article 9 GDPR provides an example of how this provision in the Draft Law regarding Specific Personal Data might be framed.

We suggest amending Article 3 to the following:

Specific Personal Data as referred to in paragraph (1) letter b includes:
- a. health data and information;
- b. biometric data;

c. genetic data;
d. sexual life/orientation;
e. political view;
f. criminal records; and
g. child data

4. Chapter III, Article 4: Rights of personal data subject

Personal Data Subject has the right to request information regarding identity clarity, fundamental legal interests, the purpose of request and usage of Personal Data, and the parties' accountability of requesting Personal Data.

Recommendation: We suggest amending Article 4 to the following:

Personal Data Subject has the right to obtain from the Personal Data Controller confirmation as to whether or not Personal Data concerning him or her are being processed, and information regarding the purposes of processing and the categories of Personal Data concerned. This right shall not adversely affect the rights and freedoms of others.

5. Chapter III, Article 5

Personal Data Subject has the right to complete their Personal Data prior to the processing by Personal Data Controller.

Recommendation: We suggest amending Article 5 to the following:

Taking into account the purposes of the processing, the Personal Data Subject has the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.

6. Chapter III, Article 6: It provides very broad individual rights to access his/her personal data - should try to specify the rights and include some exceptions.

Personal Data Subject has the right to access their Personal Data in accordance with the provisions of the legislation.

Recommendation: Personal data subject has the right to access personal data provided by them, and observed personal data, but not the personal data independently generated, derived or inferred from such data. The right to access personal data shall not apply to the extent that complying would:

- disclose trade secrets or proprietary info;
- compromise privacy, security or integrity;
- be infeasible on technical grounds or require disproportionate effort;
- require re-identifying or otherwise linking information that is not presently considered personal information.
- interfere with law enforcement, judicial proceedings, investigations
- undermine efforts to guard against, detect, or investigate malicious, unlawful, or fraudulent activity or enforce contracts
- violate federal or state laws or the rights of others
- involve technical or non-human understandable data

Where requests from the personal data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the personal data controller may refuse to act on such requests.

7. Chapter III, Article 7

Personal Data Subject has the right to update and/or correct errors and/or inaccuracies of their Personal Data in accordance with the provisions of the legislation.

Recommendation: We suggest amending Article 7 to the following:

Personal Data Subject has the right to obtain from the Personal Data Controller the rectification of inaccuracies in their Personal Data in accordance with the provisions of the legislation.

8. Chapter III, Article 8, 17(2) and 38: Personal Data Owner has the right to end processing, delete and/or destroy their Personal Data.

According to Article 8, personal Data Subject has the right to terminate the processing, to remove, and/or to delete their Personal Data.

Recommendation: Deletion rights set out in Art 8, 17(2), 38 are very broad and could cause operational issues and infeasible outcomes. Further, requirements to "terminate processing" within 3 days is also incredibly strict.

Qualitative period e.g. "reasonable notice" or something closer to 30 days for data controllers and/or processors to process withdrawal requests, given that there could be certain circumstance where data controllers and/or processors need more time to process such request or to keep processing for legitimate business interest or continuity of services (e.g. processing outstanding payment, fulfillment of services, delivery, etc). Some deletion requests cannot be fulfilled if the user intends to continue using the service.

Data controllers may deny such a request if:

(1) The personal information that the consumer requests to be deleted is necessary to:

> (A) Provide product or service requested by the consumer;
>
> (B) For the establishment, exercise, or defense of legal claims; or
>
> (C) To detect or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or identify, investigate, or prosecute those responsible for that activity.

(2) Granting such request would:

> (A) Be contrary to the public interest or the vital interests of other individuals or third parties; or
>
> (B) Conflict with other requirements of this Act or with the controller"s legal obligations

We suggest amending Article 8 to the following:

(1) Personal Data Subject has the right to obtain from the Personal Data Controller the erasure of Personal Data concerning him or her without undue delay and the Personal Data Controller shall have the obligation to erase Personal Data without undue delay where one of the following grounds applies:

> (a) the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
>
> (b) the Personal Data Subject withdraws consent on which the processing is based according to Article 18(1), and where there is no other legal ground for the processing;
>
> (c) the Personal Data have been unlawfully processed; or
>
> (d) the Personal Data have to be erased for compliance with a legal obligation to which the Personal Data Controller is subject.

(2) Paragraph 1 shall not apply to the extent that processing is necessary:

> (a) for exercising the right of freedom of expression and information;
>
> (b) for compliance with a legal obligation which requires processing by law to which the Personal Data Controller is subject or for the performanceof a task carried out in the public interest or in the exercise of official authority vested in the Personal Data Controller; or
>
> (c) for the establishment, exercise or defence of legal claims.

9. Chapter III, Article 9

Personal Data Subject has the right to withdraw their consent of processing their Personal Data that had been given to the Personal Data Controller.

Recommendation: We suggest amending Article 9 to the following:

Personal Data Subject has the right to withdraw their consent of processing their Personal Data that had been given to the Personal Data Controller. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

10. Chapter III, Article 10

Personal Data Subject has the right to submit objections to decision making actions that is only made based on automatic processing related to a person's profile (profiling).

Recommendation: We suggest amending Article 10 to the following:

If personal data is used for a decision based only on automated processing, including profiling, which has a legal or similarly significant effect with respect to housing, employment, credit, education, or insurance, the personal data subject has a right to know:

- the purpose of the decision-making;
- the principal components of personal data which were used for the decision;
- a general description of the methodology of the decision;
- a general description of the result of the decision making process.

The personal data subject may opt-out of such a decision making process or may request a review of such decisions.

This provision shall not apply if the decision:

1. is necessary for entering into, or performance of, a contract between the Personal Data Subject and a Personal Data Controller;
2. is authorised by a law to which the Personal Data Controller is subject and which also lays down suitable measures to safeguard the Personal Data Subject's rights and freedoms and legitimate interests; or
3. is based on the Personal Data Subject's explicit consent.

11. Chapter III, Article 11: Definition of 'Personal Data' to and clearly exclude Anonymized data.

"Personal Data Subject has the right to select or not selecting Personal Data processing through pseudonymization for certain purposes."

Recommendation: The Article provides broad rights to users to object to data profiling and pseudonym data processing. We suggest that users' rights to object to a certain data processing need to carefully consider the practicability of such rights. The legislation should therefore avoid framing that grants users broad and absolute rights to object, without consideration of how companies can respond to those objections. For example, by suggesting users can object to processing while still using the features/service (stopping the use of the service should be considered a valid way to object to the processing).

The right to object to processing of pseudonymised data should be removed, due to the low risk it poses to data subjects, and due to the benefits it would bring to advance the development of innovative products and services. For instance, the processing of pseudonymised health data is instrumental in providing helpful information to the public and private sector, to allow them to develop products and services that would enhance the health of a population. At the same time, processing of pseudonymized data poses low risk to individuals, as such data is no longer associated with said individuals. This is also inconsistent with GDPR.

We suggest removing Article 11 from the Bill.

12. Chapter III, Article 12: Data Subject can delay/limit personal data processing-

"Personal Data Subject has the right to delay or limit Personal Data processing proportionally in accordance with the purpose of Personal Data processing."

Recommendation: We suggest amending Article 12 to the following

Personal Data Subject has the right to obtain from the Personal Data Controller restriction of processing where one of the following applies.:

a. the accuracy of the Personal Data is contested by the Personal Data Subject, for a period enabling the Personal Data Controller to verify the accuracy of the Personal Data Controller;
b. the processing is unlawful and the Personal Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead; or
c. the Personal Data Controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Personal Data Subject for the establishment, exercise or defence of legal claims.

13. Chapter III, Article 13: Joint and several liability

"Personal Data Subject has the right to sue or receive compensation for violations of their Personal Data in accordance with the provisions of the legislation."

Recommendation: The right to "claim and receive compensation for breach of Personal Data" (Art. 13) should be removed as this suggests a tortious act without specifying mechanisms of redress, defence, due process etc. The Bill provides for data breaches under Article 40.

We suggest removing Article 13 from the Bill.

14. Chapter III, Article 14

(1) Personal Data Subject has the right to obtain and/or use their Personal Data from Personal Data Controller in the form that is in accordance with the structure and/or format commonly used or readable by electronic system or hardware used in interoperability between Electronic Systems.

(2) Personal Data Subject has the right to use and send their Personal Data to other Personal Data Controller, as long as the systems can communicate securely in accordance with the principles of Personal Data Protection based on this Law.

Recommendation: The data portability right is also overly broad. It extends to any Personal Data of the Personal Data Owner. This is not in line with data portability rights under international laws, such as the GDPR, which only extend to personal data provided by the data subject. Under the Draft Law, a Personal Data Controller would be required to disclose inferred data, which may be proprietary or commercially sensitive. This right is also not limited to data which is held electronically. For example, if a data subject requested that his or her hard copy personal information be provided, the organization would have to comply with this request by returning the personal information in a soft copy Excel spreadsheet or other machine-readable form. This could involve manually entering all hard copy data into a spreadsheet and then sharing it with the data subject. This is practically difficult to comply with. This is also exacerbated by the prescriptive, short and arbitrary timelines in the Draft Law for responding to data subject requests. These may not always align with practical realities and therefore makes compliance even more burdensome or even impractical.

We suggest amending Article 14 to the following:

Personal Data Subject shall have the right to receive personal data that they have provided in a structured, machine readable format, and the Personal Data Subject shall have the right to have the Personal Data transmitted directly from one Personal Data Controller to another, where technically feasible. Upon making a good faith effort to comply with such a request from a personal data subject to transfer the personal data they provided to the personal data subject or a third party personal data controller, the transferring personal data controller will have no further obligation or liability under the law regarding the security and/or protection of that data.

15. Chapter III, Article 16

(1) Rights of Personal Data Subject as referred to in Article 8, Article 9, Article 10, Article 11, Article, 12, and Article 14 do not apply to:

a. the national defense and security interests;
b. interests of law enforcement process;
c. public interest in the context of state administration;
d. interests of supervision of financial services, monetary, and payment systems, and financial system stability; or
e. data aggregates which processing is aimed for statistical interests and scientific research purposes in the context of state administration.

(2) Exemption as referred to in paragraph (1) is applied only in the context of implementing the provisions of the Law.

Recommendation: The Bill does not provide for reasonable limitations on data subject rights, which would align with the approach taken by GDPR. The reasonable limitations to data subject rights should be extended to all data subject rights (not just the right of access and correction), and should be expanded to include situations where they may prejudice or compromise investigations, law enforcement or legal obligations, where the requests are frivolous and vexatious, where they would reveal proprietary assets or business insights, or where giving effect to the request would require a disproportionate effort on the part of the Data Controller. The prescriptive timelines should be removed and replaced with an obligation to respond “as soon as reasonably possible” or “promptly” to allow for some flexibility while still ensuring the data controllers prioritise such requests.

We suggest amending Article 16 to the following:

(1) Rights of Personal Data Subject as referred to in Article4, Article 5, Article 6, Article 7, Article 8, Article 9, Article 10, Article 11, Article, 12, and Article 14 do not apply to:

a. the national defense and security interests that create actual physical harm;
b. interests of law enforcement process;
c. public interest in the context of state administration;
d. interests of supervision of financial services, monetary, and payment systems, and financial system stability;
e. data aggregates which processing is aimed for statistical interests and scientific research purposes in the context of state administration;
f. to the extent that complying would:

i. disclose trade secrets or proprietary info;
ii. compromise privacy, security or integrity;
iii. be infeasible on technical grounds or require disproportionate effort;
iv. require re-identifying or otherwise linking information that is not presently considered personal information;
v. interfere with law enforcement, judicial proceedings, investigations;
vi. undermine efforts to guard against, detect, or investigate malicious, unlawful, or fraudulent activity or enforce contracts
vii. violate federal or state laws or the rights of others; or
viii. involve technical or non-human understandable data.

(2) Where requests from the personal data subject under Article 4, Article 5, Article 6, Article 7, Article 8, Article 9, Article 10, Article 11, Article, 12 or Article 14 are manifestly unfounded or excessive, in particular because of their repetitive character, the personal data controller may refuse to act on such requests.

16. Chapter IV, Article 18: Consent and other bases for processing

(1) Personal Data processing as referred to in Article 17 must meet the requirement of legal consent from Personal Data Subject for one or several specific purposes that have been communicated to the Personal Data Subject.

(2) Consent as referred to in paragraph (1) is not needed in the context of Personal Data processing for the purposes of:

a. fulfillment of the agreement's obligations in the event that Personal Data Subject is one of the parties or to fulfill the request of Personal Data Subject as they do an agreement;

b. fulfillment of legal obligations by Personal Data Controller in accordance with the provisions of legislation;

c. fulfillment of vital interest protection of Personal Data Subject;

d. exercise of authority of Personal Data Controller in accordance with provisions of legislations;

e. fulfillment of Personal Data Controller's obligation in public services for public purposes; and/or

f. fulfillment of other vital interests by taking into account the purpose, needs, and balance of interests of Personal Data Controller and the rights of Personal Data Subject.

Recommendation:

The requirement for consent to be "not hidden" overlaps with the requirement in Article 19(4) for a request for consent to be clearly distinguishable from other matters, in an understandable and accessible format and to use simple and clear language. The requirements for consent to be not "by mistake, negligence or duress" import complex and subjective legal concepts, which are not commonly found in privacy laws. There are also circumstances in which implied consent may be appropriate. The requirement for consent to be "explicit" may therefore be burdensome for organizations, who will have to spend undue resources on seeking consent, and for consumers, who will be inundated with requests for consent, in circumstances in which consent is clearly implied. The Explanatory Note should be removed and the requirements for consent should be limited to those set out in Article 19.

The law should have a catch-all, more flexible basis of processing recognizing a business's "legitimate interests," for processing that presents a reasonable risk to users, or is compatible with user's expectations, to process data beyond consent. This allows consent to be more narrowly focused on key issues. These bases support key business interests like product development and improvement, security/abuse/fraud prevention, contextual advertising and associated measurement and actions such as frequency capping. A consistent interpretation/same terminology with the GDPR is highly recommended.

Therefore, we suggest amending the Article 18 to the following:

(1) Personal Data processing as referred to in Article 17 must meet at least one of the following:

a. legal consent from Personal Data Subject for one or several specific purposes that have been communicated to the Personal Data Subject.
b. fulfillment of the agreement's obligations in the event that Personal Data Subject is one of the parties or to fulfill the request of Personal Data Subject as they do an agreement;
c. fulfillment of legal obligations by Personal Data Controller in accordance with the provisions of legislation;
d. fulfillment of vital interest protection of Personal Data Subject or another natural person;
e. exercise of authority of Personal Data Controller in accordance with provisions of legislations;
f. fulfillment of Personal Data Controller's obligation in public services for public purposes; and/or
g. fulfillment of other legitimate interests by taking into account the purpose, needs, and balance of interests of Personal Data Controller and the rights of Personal Data Subject.
h. the information is publicly available
i. the collection is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the Data Subject would compromise the availability or the accuracy of the personal data;
j. the collection is necessary for evaluative purposes;
k. the personal data is collected solely for artistic or literary purposes;
l. the personal data is collected by the Data Subject's employer and the collection is reasonable for the purpose of managing or terminating an employment relationship between the organization and the Data Subject.

17. Chapter IV, Article 19: Consent has to be explicit including written or verbally recorded consent

(1) Consent to Personal Data processing is carried out through written consent or verbally recorded.
(2) Written consent as referred to in paragraph (1) can be delivered electronically or non-electronically.
(3) Written and verbally recorded consent as referred to in paragraph (1) have the same legal force.
(4) In the event that the written consent as referred to in paragraph (1) contains other objectives, the request of approval must meet the following provisions:
a. can be clearly distinguished from other things;
b. made in an understandable and easily accessible format; and
c. using simple and clear language.
(5) Consent that does not fulfill the provisions referred to in paragraph (1) to paragraph (4) is declared null and void.

Recommendation: We suggest amending Article 19 to the following:

(1) Consent to collect, use or disclose Personal Data processing is carried out through written consent, oral consent or deemed consent.
(2) Written consent as referred to in paragraph (1) can be delivered electronically or non-electronically.
(3) Written and verbally recorded consent as referred to in paragraph (1) have the same legal force.
(4) In the event that the written consent as referred to in paragraph (1) contains other objectives, the request of approval must meet the following provisions:
a. can be clearly distinguished from other things;
b. made in an understandable and easily accessible format; and
c. using simple and clear language.

(5) A Personal Data Subject is deemed to consent (as referred to in paragraph (1)) to the collection, use or disclosure of personal data about the Personal Data Subject by an Organization for a purpose if:
a. the Personal Data Subject, without actually giving written consent, voluntarily provides the personal data to the organization for that purpose; and
b. it is reasonable that the Data Subject would voluntarily provide the data.

(6) If a Personal Data Subject gives, or is deemed to have given, consent to the disclosure of personal data about the Personal Data Subject by one organization to another organization for a particular purpose, the Personal Data Subject is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organization.

18. Chapter IV, Article 20: Lack of explicit consent renders agreement null and void.

"Each agreement in which there is a Personal Data request that does not contain explicit consent from the Personal Data Subject is declared as null and void."

Recommendation: The Bill appears to set out contradictory standards around consent. "Consent" is one allowed basis for legal processing, but then Article 20 seems to require explicit consent for all processing.

It is unclear why explicit consent is required for every agreement. Legislation should recognize that there is some data processing required simply for services to function. Consent should be limited to certain specific use cases in order to ensure that basic data processing for services to function remains available. There is well documented research showing that increasing the frequency of requests for consent degrades the individual’s understanding of the importance of specific moments. This is referred to as “consent fatigue.” For example, some data processing is necessary to make products work and to ensure that they are secure and reliable. Users can generally accept and even expect and consider it reasonable that some personal information needs to be processed by a company providing a product or service. In this scenario, asking users to provide consent presents the odd decision of “agree” or “don’t use the service.” This could have the perverse effect of teaching users to simply click “agree” to everything without paying attention.

To the extent that consent is the appropriate ground for processing personal data, we urge the authority to look at substance over form when determining if consent had in fact been given by an individual.

Privacy regulations around the world recognise that different forms of consent can be valid under different circumstances. Consent can be provided in writing via a checkbox, implied by action, or by accepting a broader agreement. In some circumstances, failure to opt out could constitute valid consent. Individuals should be provided with appropriate mechanisms to exercise control that is feasible and coherent in the context of the service being provided. Example, see Singapore DPA guidelines.

We note that the draft Law also contemplates other grounds for processing in Article 18. We would like to seek more clarity on how this Article 20 interacts with Article 18 which contemplates other basis for processing. Specifically we would recommend that greater consideration be given to processing on the basis of “legitimate interests”. In many cases, legitimate interests can provide a more privacy protective standard, since it requires data controllers to balance the rights and freedoms of the individual against the interests of the organisation processing the data and justify the processing based on that test.

In totality, we therefore suggest removing Article 20 from the Bill.

19. Chapter IV, Article 22

(1) Installation of visual data processor or management tool in public places and/or in public service facilities is carried out with the following provisions:

- *a. for the purpose of security, disaster mitigation, and/or administering traffic, or collecting, analyzing, and regulating traffic Information;*
- *b. must display Information that visual data processor or management tool has been installed in the area; and*
- *c. not used to identify a person.*

(2) Provisions as referred to in paragraph (1) letter b and letter c are exempted in terms of prevention of criminal offences and law enforcement in accordance with the provisions of the legislation.

Recommendations: The Bill has an overly broad and vague prohibition of the installation of "processor or visual data processor" in public places. We would like a narrower definition of "public spaces" which currently includes private and personal spaces used for public activities. This should be limited to just "Government organised". At a minimum, we would like specificity on what constitutes "activities".

Explanatory Note for Art 22(1)): The term "public places" shall mean facilities operated by the Government, or facilities operated by private or individuals while used for Government organised activities.

20. Chapter V, Article 24: Notification requirements, with Notification within 7 days, for changes in purpose.

(1) In order to gain consent as referred to in Article 18 paragraph (1), Personal Data Controllers must submit Information on:

a. legality of processing Personal Data;
b. purpose of processing Personal Data;
c. types and relevance of Personal Data to be processed;
d. retention period of document containing Personal Data;
e. details on the collected Information;
f. period of Personal Data processing; and
g. rights of Personal Data Subject.

(2) In processing Personal Data, Personal Data Controller is required to show consent evidence that has been given by Personal Data Subject.

(3) In the event of Information change as referred to in paragraph (1), Personal Data Controller is required to notify Personal Data Subject no later than 7 x 24 hours (seven times twenty four hours) after the change of Information.

Recommendation: The key challenge with this provision is that the elements to be notified are too vague to be actionable and are not likely to be relevant to people. The Bill should instead adopt the elements to be notified as per the EU Article 29 Working Party Guidelines on consent under Regulation 2016/679. In particular, the phrases "relevance of data," "retention period of the documents containing such data," "details on data collection", and "data processing timeline" should be clarified and narrowed.

Instead of requiring data controllers to show "evidence of consent," the Bill should follow GDPR, which states: "the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data".

The 7-day timelines for updating Personal Data Owners of any changes is unrealistic and not helpful for people.

Under this standard, companies, which make changes to their processing activities on a regular basis, would end up providing constant notifications to people. To avoid overwhelming people with notifications, this provision should be revised to only require notification of "material" changes to processing activities.

Privacy notifications is an area where industry and government can work together – finding practical approaches to notice & consent, that the ordinary user will appreciate.

We suggest amending the Article 24 to the following:

(1) In order to gain consent as referred to in Article 18 paragraph (1), Personal Data Controllers must submit Information on:
   a. purpose of processing Personal Data For which consent is sought;
   b. types of Personal Data to be processed;
   c. rights of Personal Data Subject to withdraw consent.

(2) In processing Personal Data based on consent, Personal Data Controller must be able to demonstrate that consent has been given by Personal Data Subject.
(3) In the event of a material change toInformation as referred to in paragraph (1), Personal Data Controller is required to notify Personal Data Subject without delay after the material change of Information.

21. Article 25: Requirements for processing withdrawal of consent in 3 days

(1) Personal Data Controller is required to withdraw their Personal Data processing in the case Personal Data subject withdraws consent on processing Personal Data.
(2) Termination of Personal Data processing as referred to in paragraph (1) shall be made no later than 3 x 24 hours (three times twenty four hours)

Recommendation: Firstly the link between Article 9 and Article 25 should be clarified to avoid confusion and overlap. The rigid time frame for compliance in Article 25 should be removed.

We suggest amending the Article 25 to the following:

(1) Personal Data Controller is required to cease Personal Data processing in the case Personal Data subject withdraws consent on processing Personal Data in accordance with Article 9
(2) Termination of Personal Data processing as referred to in paragraph (1) shall be made as soon as reasonably practicable from the date the Personal Data Controller receives a request of consent withdrawal of Personal Data processing.

22. Chapter V, Article 26:

- **New provision on Suspension (delay) and stop (limit) processing, to be done within 2 days.**
- **Exemptions are a short list and includes situations where "Data Subjects are contractually bound".**

(1) Personal Data Controller is required to delay and limit Personal Data processing either in partially or completely no later than 2 x 24 (two times twenty four) hours from the date Personal Data Controllers receive the request of delay and limitation of Personal Data processing.

(2) Delay and limitation of Personal Data processing as referred to in paragraph (1) are exempted in terms of:

   a. there are provisions of legislations that do not allow delay and
   b. limitation of Personal Data processing;
   c. could harm the safety of others; and/or
   d. Personal Data Subject is bound to written agreement that does not allow delay and limitation of Personal Data processing.

Recommendation: The link between Article 12 and Article 26 should be clarified to avoid confusion and overlap. The rigid timeline for compliance should also be removed.

We suggest amending the Article 26 to the following:

(1) Where the Personal Data Owner has made a request to restrict the processing of his or her Personal Data under Article 12, the Personal Data Controller is required to give effect to such request either partially or completely as soon as reasonably possible after the Personal Data Controller receives the request of delay and limitation of Personal Data processing where one of the following bases applies:

   a. the accuracy of the personal data is contested by the data subject, for a period enabling the Personal Data Controller to verify the accuracy of the personal data;
   b. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
   c. the Personal Data Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;
   d. the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the Personal Data Controller override those of the data subject.

(2) Restriction of Personal Data processing as referred to in paragraph (1) are exempted if

   a. there are provisions of legislations that do not allow restriction of Personal Data processing;
   b. such restriction could harm the safety of others; and/or
   c. Personal Data Subject is bound to written agreement that does not allow restriction of Personal Data processing.

23. Chapter V, Article 31:

- ***Requirement to record all activities***
- ***Personal Data Controllers must record all activities of Personal Data processing.***

Personal Data Controllers must record all activities of Personal Data processing.

Recommendation: We suggest removing the Article 31 from the Bill

24. Chapter V, Article 32:

(1) Personal Data Controller is required to provide access to the Personal Data Subject for Personal Data being processed and the Personal Data processing track record in accordance with the period of storage of Personal Data.

(2) Access as referred to in paragraph (1) shall be granted no later than 3 x 24 (three times twenty four) hours from the date the Personal Data Controller receives a request for access.

Recommendation: We suggest removing the Article 32 from the Bill

25. Chapter V, Article 33:

Personal Data Controllers shall not give access to changes to Personal Data to the Personal Data Subject in the event that it is known or duly suspected:

a. endanger the security or physical health or mental health of Personal Data Subject and/or other people's;
b. impacting to the disclosure of other people's Personal Data; and/or
c. against the national defense and security interests.

Recommendation: The interaction between Article 33 and Article 4 should be clarified to avoid overlap and confusion.

We suggest amending the Article 33 to the following:

Personal Data Controllers shall not give access to changes to Personal Data to the Personal Data Subject under Article 4 in the event that it is known or duly suspected to:

a. endanger the security or physical health or mental health of Personal Data Subject and/or other people's;
b. impacting to the disclosure of other people's Personal Data; and/or
c. against the national defense and security interests.

26. Chapter V, Article 34: Accuracy and Correction, with response within "24 hours"

(1) Personal Data Controllers must update and/or correct errors and/or inaccuracies of Personal Data at least 1 x 24 (one times twenty four) hours from the time Personal Data Controllers receive the request of update and/or correction of Personal Data.

(2) Personal Data Controller is required to notify the result of update and/or correction of Personal Data to the Personal Data Subject.

Recommendation: The interaction between Article 7 and Article 34 needs to be clarified. Furthermore, the rigid time frame for compliance should be removed.

We suggest amending the Article 34 to the following:

(1) Personal Data Controllers must update and/or correct errors and/or inaccuracies of Personal Data as requested under Article 7 as soon as reasonably possible after the time Personal Data Controllers receive the request of update and/or correction of Personal Data.
(2) Personal Data Controller is required to notify the result of update and/or correction of Personal Data to the Personal Data Subject.

27. Chapter V, Article 35: Data controller is required to guarantee data accuracy, completion and consistency, by conducting data verification

(1) Personal Data Controllers must guarantee the accuracy, completeness, and consistency of Personal Data in accordance with the provisions of the legislation.
(2) In guaranteeing the accuracy, completeness, and consistency of Personal Data as referred to in paragraph (1) Personal Data Controllers are required to do verifications.

Recommendation:
There should not be an absolute requirement to "guarantee" the accuracy, completeness and consistency of Personal Data. Instead, Personal Data Controllers should be considered compliant if the Personal Data Owner has the opportunity to access their data (and therefore verify its accuracy) and the Personal Data Controller takes reasonable steps to correct inaccurate Personal Data. The Bill, through Art. 4 and 7, provides for these rights of access and correction.

Paragraph (2) requires the Personal Data Controller to carry out verification in order to guarantee the accuracy, completeness, and consistency of Personal Data. This verification requirement is vague and it is not clear what "verification" entails. There should not be an obligation on the Personal Data Controller to proactively monitor and verify Personal Data. Paragraph (2) should be removed.

Assuming that what Article 35 (2) indeed requires is for data controllers to verify the identity of data subjects whose data they process, this would require the collection of proofs of identity, such as one's national ID card. This is in contravention of the principle of data minimization, which can be seen in international privacy benchmarks, such as GDPR. This principle states that where personal data is needed, it should be adequate, relevant, and limited to what is necessary for the purpose. The collection of proofs of identity to verify one's identity is not always necessary for the purpose of delivering a service, such as the use of an online platform. As such, the requirement to verify the identity of data subjects should be removed.

There needs to be a reasonable threshold on a data controller's efforts to maintain data accuracy by giving into consideration the tradeoff between the amount of data collected and levels of data accuracy. In certain cases, maintaining a high level of data accuracy would require more data to be collected and this can create more privacy implications. Data Controller may be expected to provide "a reasonable effort to ensure the accuracy and completeness of personal data" instead of a guarantee. We therefore seek clarity on who this applies to and suggest more focus on transparency and control mechanisms.

We suggest amending Article 35 to the following:

(1) Personal Data Controllers must take reasonable steps to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified,in

accordance with the provisions of the legislation.

28. Chapter V, Article 37:

(1) Personal Data Controllers must end Personal Data processing when:

a. have reached the retention period;

b. purposes of Personal Data processing have been achieved; or

c. there is a request from Personal Data Subject.

(2) Termination of Personal Data processing as referred to in paragraph (1) is carried out in accordance with the provisions of the legislation.

Recommendation: Article 37 is very broadly drafted and needs to be narrowed and clarified. In particular, paragraph (a) should be removed as the Bill does not prescribe a retention period. The period for which data is retained will depend on the purpose for which it is being processed (which is covered by paragraph (b)). Paragraph (c) should also be removed as the Personal Data Subject already has a right to erasure under Article 8, a right to withdraw consent under Article 9 and a right to restrict processing under Article 12.

We suggest amending Article 37 to the following:

(1) Personal Data Controllers must end Personal Data processing when:

a. purposes of Personal Data processing have been achieved;

(2) Termination of Personal Data processing as referred to in paragraph (1) is carried out in accordance with the provisions of the legislation.

29. Chapter V, Article 38

(1) Personal Data Controllers must delete Personal Data processing when:

a. Personal Data is no longer needed to achieve the purpose of Personal Data processing;

b. Personal Data Subject has withdrawn their consent on Personal Data processing;

c. there is a request from Personal Data Subject; or

d. Personal Data is obtained and/or processed in an illegal manner.

(2) Personal Data Deletion as referred to in paragraph (1) is carried out in accordance with the provision of the legislation.

(3) Personal Data that has been deleted as referred to in paragraph (1) can be recovered/re-displayed in its entirety in the event of a written request from Personal Data Subject.

(4) Request as referred to in paragraph (3) may be submitted as long as it has not passed the retention period in accordance with the provisions of the legislation.

Recommendation: Paragraph (b) should be removed as it overlaps with Articles 9 and 25. Paragraph (c) should be removed as it overlaps with the right to erasure under Article 8.

Paragraphs (3) and (4) should also be removed as the obligation to recover or visually display deleted data is not technically feasible once the data has been deleted.

We suggest amending Article 38 to the following:

(1) Personal Data Controllers must delete Personal Data processing when:
   a. Personal Data is no longer needed to achieve the purpose of Personal Data processing;
   b. Personal Data is obtained and/or processed in an illegal manner.

(2) Personal Data Deletion as referred to in paragraph (1) is carried out in accordance with the provision of the legislation.

30. Chapter V, Article 39

(1) Personal Data Controllers must destroy Personal Data when:
   a. no longer has use value;
   b. retention period has expired and annotated as destroyed based on the archive retention schedule;
   c. there is a request from Personal Data Subject; or
   d. unrelated to completion of the legal process of a case.

(2) Personal Data Destruction as referred to in paragraph (1) is carried out in accordance with the provisions of the legislation.

Recommendation: Article 39 should be removed as it overlaps with the obligation to delete Personal Data under Article 38.

We suggest following the new definition of Personal Data Breach (adopted from GDPR): Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

31. Article 40: Data breach notification provision.

(1) In the event of failure to protect Personal Data, the Personal Data Controller must submit a written notice within no later than 3 x 24 (three times twenty four) hours to:
   a. Personal Data Subject; and
   b. Minister

(2) Notification in writing as referred to in paragraph (1) contains:
   a. Disclosed Personal Data;
   b. when and how Personal Data is disclosed; and
   c. efforts to handle and recover the disclosure of Personal Data by Personal Data Controllers.

(3) *In certain issues the Personal Data controller is obliged to notify the society regarding the failure of protecting Personal Data.*

Recommendation: The Bill should take a risk-based approach to notifications and apply the breach notification requirement only to breaches that are likely to threaten real and significant harm to the Personal Data Owners involved. If a harm-based standard is not applied, data owners and regulators are likely to be deluged with breach notifications for even minor breaches that do not materially affect them. People are likely to ignore such notifications, thereby failing to act on notifications that do impact them. At the same time, regulators will have a hard time processing and responding to a lot of breach notifications - even those that do not pose a material risk. Regulators should focus their limited resources on breaches that actually harm people; as such, it is necessary to require breach notifications only in instances where the incident is likely to threaten real and significant harm to personal data owners.

We strongly recommend a clear threshold for data breach notification. Unclear threshold will lead to uncertainty and unnecessary burdens for the regulators and businesses. Applying a concept of "significant harm" or "serious harm" threshold to breach notifications helps to ensure regulators have visibility into the incidents that pose actual risk to users and ensures regulators will be able to focus guidance and oversight activities where they are most needed.

However, if the threshold for 'harm' is too low. It could result in over-notification to the regulator and to individuals. It is also appropriate to provide more certainty to agencies and to better align with other countries which have a higher threshold for when privacy breaches should be notified.

Therefore, breaches should be defined as a breach of security that leads to unauthorized third-party acquisition of data. The trigger for legal requirement to notify regulators or users of a data breach should be based on a materiality threshold that looks at the impact of the breach on the affected data subjects, such as:

- Introducing a clear threshold for breach notifications based on level of "harms".
- Identifying specific types of data that inherently pose a risk to users if subject to breach. (e.g. financial information, or information that directly enables identity theft such as National ID)

The Bill should also clarify the meaning of "failure of Personal Data protection". This phrase is very broad and could also lead to a deluge of breach notifications. The notification obligation should only be triggered where there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (as is the case under GDPR).

The timeline for notification should be amended to "without undue delay" after becoming aware of the breach instead of within "3 x 24 hours". Requiring notifications on short timelines can delay a company's efforts to investigate and stop the data breach, as well as interfere with ongoing law enforcement investigations.

Furthermore, the Bill should only obligate notification to the regulator and affected individuals only, rather than the public at large in special cases.

We suggest amending the Article 40 to the following:

(1) In the event of Personal Data Breach which is likely to result in serious harm to Personal Data Subjects, the Personal Data Controller must submit a written notice without undue delay after having become aware of the Personal Data Breach

a. Minister; and
b. if the Personal Data Subject is able to take steps to minimize the negative effects of the Personal Data Breach, to such Personal Data Subject

(2) Notification in writing as referred to in paragraph (1) contains:

a. Disclosed Personal Data;
b. when and how Personal Data is disclosed; and
c. efforts to handle and recover the disclosure of Personal Data by Personal Data Controllers.

(3) The notification referred to in paragraph 1 shall not be required if any of the following conditions are met:

a. The Personal Data Controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the Personal Data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
b. The Personal Data Controller has taken subsequent measures which ensure that the high risk of serious harm to Personal Data Subjects referred to in paragraph 1 is no longer likely to materialize;
c. In the case of notification to individual Personal Data Subjects, it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the Personal Data Subjects are informed in an equally effective manner.

32. Chapter V, Article 42

(1) Obligations of Personal Data Controller as referred to in Article 32, Article 34, Article 37, Article 38 paragraph (1) letter a, letter b, and letter c, Article 39 paragraph (1) letter c, and Article 40 paragraph (1) letter a, do not apply to:

a. the importance of national defense and security;
b. interests of law enforcement process;
c. public interest in the context of state administration;
d. interests of supervision of financial services, monetary, and payment systems, and financial system stability; or
e. data aggregates which processing is aimed for statistical and scientific research purposes in the context of state administration.

(2) Exemption as referred to in paragraph (1) is applied only in the context of implementing the provisions of the Law.

Recommendations: We would like clarification that these provisions do *not* mandate any sharing with the Government for any reason, including law enforcement, for public interest purposes. The Bill should not defer to subsequent regulations around these exclusions.

We would also suggest a clearer and more specific definition of "public interest" in the context of state administration, to ensure certainty in the application of the law.

We suggest amending Article 42 to the following:

(1) Obligations of Personal Data Controller as referred to in Article 32, Article 33, Article 34, Article 36, Article 37, Article 38 paragraph (1) letter a, letter b, and letter c, Article 39, and Article 40 paragraph (1) letter a, do not apply to:
   a. the importance of national defense and security;
   b. interests of law enforcement process;
   c. public interest in the context of state administration;
   d. interests of supervision of financial services, monetary, and payment systems, and financial system stability; or
   e. data aggregates which processing is aimed for statistical and scientific research purposes in the context of state administration.

33. Chapter V, Article 43 – Personal Data Processor obligations

(1) In the event Personal Data Controller appoints Personal Data Processor, Personal Data Processor is required to process Personal Data based on the instruction or order of Personal Data Controller unless otherwise specified in accordance with provisions of the legislation.
(2) Personal Data processing as referred to in paragraph (1), is carried out by taking into account the provisions of Personal Data processing in accordance with this Law.
(3) Personal Data processing as referred to in paragraph (1) is included in the responsibility of Personal Data Controller.
(4) In the event of Personal Data Processor carried out Personal Data processing outside the instruction or order and purposes specified by Personal Data Controller, Personal Data processing is the responsibility of Personal Data Processor.

Recommendation: We suggest amending the Article 43 to the following:

(1) In the event Personal Data Controller appoints Personal Data Processor, Personal Data Processor is required to process Personal Data based on the instruction or order of Personal Data Controller unless otherwise specified in accordance with provisions of the legislation.
(2) Personal Data processing as referred to in paragraph (1), is carried out by taking into account the provisions of Personal Data processing in accordance with this Law.
(3) Personal Data processing as referred to in paragraph (1) is included in the responsibility of Personal Data Controller.
(4) In carrying out the instructions of the Personal Data Controller, the Personal Data Processor is required to apply reasonable technical and organizational standards to protect the rights of data subjects.
(5) In carrying out Personal Data processing, Personal Data Processor is required to maintain Personal Data confidentiality.

34. Chapter V, Article 44 – specific processor obligations for confidentiality; security; supervision of parties; protection; prevention of unauthorized access; maintain a record of all activities; accuracy, completeness and consistency.

The obligations as referred to in Article 21 paragraph (1), Article 27, Article 28, Article 29, Article, 30, Article 31, and Article 35 also applies to Personal Data Processor.

Recommendation: We suggest removing the Article 44 from the Bill.

35. Chapter V, Article 45

(1) In certain issues Personal Data Controller and Personal Data Processor shall appoint an official or officer who carries out the Personal Data protection function.

(2) In certain issues as referred to in paragraph (1) includes:

- *a. personal Data processing for the interests of public services;*
- *b. the core activities of the Personal Data Controller have the nature, scope, and/or objectives that require regular and systematic monitoring against large-scale Personal Data; and*
- *c. the core activities of the Personal Data Controller consist of large-scale processing of specific Personal Data*
- *d. and/or Personal Data relate to criminal acts.*

(3) Officials/officers carrying out Personal Data protection function as referred to in paragraph (1) shall be appointed based on professional qualities, knowledge on law and Personal Data protection practices, and the ability to fulfill their duties.

(4) Officials or Officers who carry out Personal Data protection as referred to in paragraph (3) may originate from within and/or outside the Personal Data Controller or Personal Data Processor.

Recommendation: The Bill should clarify the criteria for organisations to appoint data protection officers.

We suggest amending Article 45 to the following:

(1) In the circumstances specified in paragraph (2), the Personal Data Controller and Personal Data Processor shall appoint an official or officer who carries out the Personal Data protection function.

(2) The circumstances referred to in paragraph (1) are:

- a. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- b. the core activities of the Personal Data Controller or Personal Data Processor consist of processing operations which, by virtue of their nature, scope, and/or purposes require regular and systematic monitoring of Personal Data Subjects on a large scale; and
- c. the core activities of the Personal Data Controller or Personal Data Processor consist of large-scale processing of Specific Personal Data and/or Personal Data related to criminal convictions and offences.

(3) Officials/officers carrying out Personal Data protection function as referred to in paragraph (1) shall be appointed based on professional qualities, knowledge on law and Personal Data protection practices, and the ability to fulfil their duties.

(4) Officials or Officers who carry out Personal Data protection as referred to in paragraph (3) may originate from within and/or outside the Personal Data Controller or Personal Data Processor.

36. Article 49: Cross-border Transfers provisions

(1) Personal Data Controllers can transfer Personal Data to other Personal Data Controllers outside the jurisdiction of the Republic of Indonesia in terms of:

a. the country where Personal Data Controller is located or international organization that receives transfer of Personal Data has a level of Personal Data protection which is equal or higher than what is stipulated in this Law;
b. there is an appropriate safeguard of Personal Data.
c. there is an international agreement between countries; and/or
d. there are other conditions based on the interests of Personal Data Subject.

(2) Further provisions regarding Personal Data transfer as referred to in paragraph (1) are regulated in Government Regulation.

Recommendation: The Bill should clarify that consent is one basis for transfer but is not required for all transfers, in line with the ASEAN Cross Border Privacy Rules Framework and OECD Privacy Principles.

The Bill should leverage international data transfer standards and contracts to ensure that the Bill is interoperable with global standards (the APEC Cross-Border Privacy Rules offer a multilateral cross-border data transfer framework that Indonesia can consider joining). An example would be Article 24 of Japan's APPI, which imposes restrictions on the transfer of personal information of Japanese citizens to third parties in foreign countries except when a third party has established a system which meets the Rules of the Commission to "continuously implement equivalent necessary measures." These regulations for implementing Article 24 specifically call out a company's APEC Cross Border Privacy Rules (CBPR) certification as satisfying this requirement. The Bill should also include certifications as mechanisms for ensuring that data is transferred in accordance with high privacy standards. Under such an approach, a data controller that demonstrates to an independent third party certifier that it complies with specific requirements should be allowed to transfer data outside of Indonesia without consent of the individual or by relying on another method.

We would also like to seek clarification on the standards to be used and if such standards have an alignment with a particular international standard. We recognize the importance of balancing personal data protection and cross-border data flow. Therefore, we encourage the government to use an international standard of data protection as a reference.

Expanding the number of legal bases which allow international transfer that is more aligned with international norms and harmonised with global data governance frameworks, doesn't hinder international trade. This may include adding grounds on why a cross border data flow is allowed based on:

- Exception for personal data that is contained within a single company, where there are baseline privacy and security standards that apply regardless of the location of the data
- Binding Corporate Rules between an affiliate group of companies
- Contractual Necessity: the transfer is necessary for the performance of a contract between the organisation and the individual
- Interest of the individual: the transfer is necessary for the conclusion or performance of a contract between the organisation and a third party which is entered into at the individual's request, or which a reasonable person would consider to be in the individual's interest;
- Necessary to respond to an emergency that threatens the life, health or safety of an individual.

We therefore, suggest amending the Article 49 to the following:

(1) Personal Data Controllers can transfer Personal Data to other Personal Data Controllers outside the jurisdiction of the Republic of Indonesia if at least one of the following factors applies:

a. the country where Personal Data Controller or Personal Data Processor is located has a level of Personal Data protection which is equal or higher than what is stipulated in this Law;
b. there is a contract with the Personal Data Controller or Personal Data Processor that has an appropriate safeguard of Personal Data;
c. there is an international agreement between countries; and/or
d. The Data Subject has consented to the transfer;
e. There are applicable binding corporate rules regarding personal data protection between members of a corporate group the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
f. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Personal Data Subject between the Personal Data Controller and another natural or legal person;
g. the transfer is necessary for important reasons of public interest; the transfer is necessary for the establishment, exercise or defense of legal claims; or
h. the transfer is necessary in order to protect the vital interests of the Personal Data Subject or of other persons, where the Personal Data Subject is physically or legally incapable of giving consent.
i. there are other conditions based on the interests of Personal Data Subject.

(2) Further provisions regarding Personal Data transfer as referred to in paragraph (1) are regulated in Government Regulation.

37. Chapter VIII, Article 51: Individuals are prohibited from obtaining or collecting personal data that does not belong to them with the intention of unlawfully benefiting themselves or causing harm to personal data subject

(1) Individuals are prohibited from obtaining or collecting Personal Data that does not belong to them with the intention to unlawfully benefit themselves or other people or may cause harm to Personal Data Subject.
(2) Individuals are prohibited from unlawfully disclosing Personal Data that does not belong to them.
(3) Individuals are prohibited from unlawfully using Personal Data that does not belong to them.

Recommendation: We suggest amending the Article 51 to the following:

(1) Individuals that act as Personal Data Controllers or Personal Data Processors must comply with their respective obligations under this Law except that the following are exempted from the scope of this Law:

a. any individual acting in a personal or domestic capacity; or
b. any employee acting in the course of his employment with an organization;
c. any other circumstance stipulated by regulation.

38. Chapter VIII, Article 54

(1) Individuals are prohibited from falsifying Personal Data with the intention to benefit themselves or other people or that can cause harm to others.
(2) Individuals are prohibited to sell or purchase Personal Data.

Recommendation: The Bill provides for an overly broad and vague prohibition on, and definition of, the sale of data.

The term "sale" of data should be clarified, and a proper definition added, to ensure that the Bill does not inadvertently prohibit standard advertising. We note that the addendum states that "The term sell or purchase the Personal Data excludes monetization of Personal Data" However, to ensure clarity, we recommend that "sale" be explicitly defined in the Act as

A clearer definition of "sale" might be framed as, "the exchange of personal data for monetary consideration by the data controller to a person for the person to license or sell the covered information to additional persons".

We suggest amending Article 54 to the following:

(1) Individuals are prohibited from falsifying Personal Data with the intention to benefit themselves or other people or that can cause harm to others.
(2) Individuals are prohibited from exchanging Personal Data for monetary consideration so that the recipient of the Personal Data can licence or sell the Personal Data to additional individuals.

39. Chapter XIII

- **Penalty Provisions (Articles 61 – 69)**
- **Provisions include “individuals” – and could extend to individual and employee liability.**
- **Criminal penalties are retained – including for intentional unlawful collection, use and disclosure; unlawful operation/use of CCTVs;**

Article 61:

(1) Individuals who intentionally obtain or collect Personal Data that does not belong to them with the intention to unlawfully benefit themselves or others or may cause loss to Personal Data Subject as referred to in Article 51 paragraph (1) shall be liable to imprisonment of a maximum of 5 (five) years or a fine worth Rp50,000,000,000 (fifty billion rupiah).

(2) Individuals who intentionally and unlawfully disclose Personal Data that does not belong to them as referred to in Article 51 paragraph (2) is liable to imprisonment of a maximum of 2 (two) years or a fine worth Rp20,000,000,000 (twenty billion rupiah).

(3) Individuals who intentionally and unlawfully use Personal Data that does not belong to them as referred to in Article 51 paragraph (3) is liable to imprisonment of a maximum of 7 (seven) years or a fine worth Rp70,000,000,000 (seventy billion rupiah).

Recommendation:

While it is important to have a robust enforcement framework, it is critical that this not stifle business and innovation for fear of penal sanctions.

Imposing criminal liability on defaulting data controllers is out of step with international data protection regulations. Imprisoning individuals for violating data protection regulations is excessive in light of alternative punishment approaches that are available. The potential for actual imprisonment for data protection violations will result in many companies avoiding Indonesia as a potential market, a result that would be detrimental to foreign investments. By placing over-reliance on criminal punitive measures, the Bill ignores opportunities to strengthen enforcement and adopt other means to prevent harm.

The Bill should implement an enforcement strategy that focuses on better data breach detection by fostering trust between a regulator and the regulated, promoting accountability mechanisms through codes of practice, and cautiously using punitive sanctions as a last resort. The Regulator should also operate as a mediator to enable more efficient data protection mechanisms to fiduciaries and processors. An enduring participatory enforcement strategy is not possible when the law leans more to deterrence and punitive measures.

On this basis, the personal criminal liability for managers and controlling personnel of a corporation should be removed.

Criminal penalties should be removed for the breaches listed. Criminal liability should only imposed for deliberate, repeated or egregious breaches that result in tangible, measurable harm due to the misdeeds of malicious actors and applied on a graduated basis.

Warnings, administrative fines and other clearly structured civil measures should be used to foster compliance instead. These will help to maximise voluntary compliance with the Bill.

Additionally, the higher penalties for organizations should be removed as these are arbitrary.

We suggest amending the Article 61 to the following:

(1) Individuals who intentionally obtain or collect Personal Data that does not belong to them with the intention to unlawfully benefit themselves or others or may cause loss to Personal Data Subject as referred to in Article 51 paragraph (1) shall be liable to a fine worth Rp50,000,000,000 (fifty billion rupiah).
(2) Individuals who intentionally and unlawfully disclose Personal Data that does not belong to them as referred to in Article 51 paragraph (2) is liable to a fine worth Rp20,000,000,000 (twenty billion rupiah).
(3) Individuals who intentionally and unlawfully use Personal Data that does not belong to them as referred to in Article 51 paragraph (3) is liable a fine worth Rp70,000,000,000 (seventy billion rupiah).

Article 62:
Individuals who intentionally and unlawfully install and/or operate a visual data processor or management tool in public facilities or public service facilities that may threaten or violate the Protection of Personal Data as referred to in Article 52, is liable to imprisonment of a maximum of 1 (one) year or a fine worth Rp10,000,000,000 (ten billion rupiah).

Recommendation: We suggest amending the Article 62 to the following:

Individuals who intentionally and unlawfully install and/or operate a visual data processor or management tool in public facilities or public service facilities that may threaten or violate the Protection of Personal Data as referred to in Article 52, is liable to a fine worth Rp10,000,000,000 (ten billion rupiah).

Article 63:
Individuals who intentionally and unlawfully use visual data processor or management tool in public facilities or public service facilities that is used to identify a person as referred to in Article 53, is liable to imprisonment of a maximum of 1 (one) year or a fine worth Rp10,000,000,000 (ten billion rupiah).

Recommendation: We suggest amending the Article 63 to the following:

Individuals who intentionally and unlawfully use visual data processor or management tool in public facilities or public service facilities that is used to identify a person as referred to in Article 53, is liable to fine worth Rp10,000,000,000 (ten billion rupiah).

Article 64:
(1) Individuals who intentionally falsify Personal Data with the intention to benefit themselves or others or that can cause harm to others as referred to in Article 54 paragraph (1) is liable to imprisonment of a maximum of 6 (six) years or a fine worth Rp60,000,000,000 (sixty billion rupiah).

(2) Individuals who intentionally sell or purchase Personal Data as referred to in Article 54 paragraph (2) is liable to imprisonment of a maximum of 5 (five) years or a fine worth Rp50,000,000,000 (fifty billion rupiah).

Recommendation: We suggest amending the Article 64 to the following:

(1) Individuals who intentionally falsify Personal Data with the intention to benefit themselves or others or that can cause harm to others as referred to in Article 54 paragraph (1) is liable to a fine worth Rp60,000,000,000 (sixty billion rupiah).
(2) Individuals who intentionally sell or purchase Personal Data as referred to in Article 54 paragraph (2) is liable to a fine worth Rp50,000,000,000 (fifty billion rupiah).

Article 65:
In addition to the criminal sentence as referred to in Article 61 to Article 64, the defendant can also be sentenced to additional punishment in the form of deprivation of income and/or assets obtained or proceeds of criminal offenses and compensation.

Recommendation: We suggest removing the Article 65 from the Bill.

Article 66:

(1) In the case of a criminal act as referred to in Article 61 to Article 64 is committed by a Corporation, punishment may be imposed on caretaker, control holder, order giver, benefit holder, and/or Corporation.
(2) Punishment that can be imposed on Corporation are only criminal fines.
(3) Criminal fine imposed on Corporation is no more than 3 (three) times of the maximum criminal fine being sentenced.
(4) In addition to being fined as referred to in paragraph (2), Corporation may be subject to additional punishment in the form of:
  a. deprivation of income and/or assets obtained or proceeds from criminal offences;
  b. to freeze some or the whole Corporation's business;
  c. permanent prohibition of certain actions;
  d. termination of some or all locations of Corporation business or business activities;
  e. carry out obligations that have been neglected; and f. payment of compensation.

Recommendation: We suggest amending the Article 66 to the following:

(1) Punishment that can be imposed on Corporation are only criminal fines;

We also recommend deleting Article 66 (1) (3) (4)

Article 67:

(1) *If the court handed down a fine penalty verdict, the convict is given 1 (one) month period after the verdict has obtained permanent legal force to pay the fine.*

(2) *In the case of strong reasons, the period as referred to in paragraph (1) may be extended for a maximum period of 1 (one) month.*

(3) *Should the convict did not pay the fine penalty within the period referred to in paragraph (1) or paragraph (2), their assets or income can be confiscated and auctioned by the Prosecutor to pay for the unpaid fine penalty.*

(4) *Should confiscation and auction of assets or income as referred to in paragraph (3) is inadequate or impossible to carry out, the unpaid fine penalty is replaced with the longest imprisonment penalty for the relevant crime.*

(5) *The length of imprisonment as referred to in paragraph (4) is determined by the Judge and is included in the court's decision.*

Recommendation: We suggest removing Article 67 from the Bill.

Article 68:

(1) *In the case of confiscation and auction of assets or income as referred to in Article 67 paragraph (4) imposed on the convicted Corporation is inadequate to pay for the fee penalty, the Corporation is subject to a substitute penalty in the form of freezing some or the whole the Corporation's business activities for a maximum period of 5 (five) years.*

(2) *The freezing duration of some parts or the whole Corporation's business activity as referred to in paragraph (1) is determined by the Judge and included in the court's decision.*

Recommendation: We suggest removing Article 68 from the Bill.

40. Chapter XV, Article 71

When this Law comes into force, all laws and regulations that are implementing regulations concerning Personal Data Protection are declared as still valid as long as it does not conflict with the provisions in this Law.

Recommendation: We recommend that the interaction between the Bill and other laws, such as GR-80 be clarified. If there is a conflict between the Bill and other laws, the Bill should prevail to the extent of the inconsistency, as the Bill should function as Indonesia's comprehensive privacy law.

We suggest amending Article 71 to the following:
When this Law comes into force, all laws and regulations that are implementing regulations concerning Personal Data Protection are declared as still valid as long as it does not conflict with the provisions in this Law. If such laws and regulations do conflict with the provisions of this Law, the provisions of this Law shall prevail to the extent of such inconsistency.

41. Comments on Independent regulatory authority

The Bill does not establish an independent commission to regulate and oversee privacy matters. Furthermore, there are several Articles in the Privacy Bill that reference the fact that different sectoral regulators may issue their own regulations relating to personal data processed by organisations in those sectors.

It would be necessary to have a dedicated department within the MCIT or an independent institution that will govern personal data-related matters. This can be achieved by consolidating oversight into one independent and central commission.

Such an approach would be consistent with most international benchmarks.

Indonesia should, for instance, consider the model of the Singapore PDPC when constituting its DPA, especially due to the PDPC's dual-mandate of ensuring both data protection and data innovation.

As an example, the PDPC has been a leader in terms of employing innovative regulatory approaches, such as regulatory sandboxes, which allows it to working with companies to identify and solve challenges presented by new technologies and data protection regulation. In particular, the PDPC has conducted several "regulatory sandbox" exercises that allow co-created policy solutions.

Although it is critical to have an independent DPA, apart from that, there is no one ideal model for a DPA. Rather, governments should consider a range of factors depending on their size and resources, and learn from the successes and challenges encountered by various data protection authorities worldwide.[1]

42. CHAPTER XIA

A. Article 57A, Personal Data Protection Commission

(1) The Ministry shall establish the Personal Data Protection Commission.
(2) The Personal Data Protection Commission is responsible for the administration of this Law.
(3) The Personal Data Protection Commission may appoint one or more advisory committees to provide advice to the Personal Data Protection Commission with regard to the performance of any of its functions under this Law.
(4) The Personal Data Protection Commission may consult such advisory committees in relation to the performance of its functions and duties and the exercise of its powers under this Law but shall not be bound by such consultation.
(5) The Personal Data Protection Commission may appoint, by name or office, from among public officers and employees:

a. the Commissioner for Personal Data Protection; and
b. such a number of Deputy Commissioners for Personal Data Protection, Assistant Commissioners for Personal Data Protection and inspectors, as the Personal Data Protection Commission considers necessary.

[1] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement.pdf

(6) The formation, structure and funding of the Personal Data Protection Commission should also be considered following stakeholder inputs.

B. Article 57B: The Personal Data Protection Commission shall have the following role and functions:
   a. to act as the lead agency in the public sector in respect of the functions specified in subsections b. to l. below;
   b. to promote awareness of Personal Data protection in the Republic of Indonesia;
   c. to provide consultancy, advisory, technical, managerial or other specialist services relating to personal data protection;
   d. to work with and advise the Government and any other public sector body on national needs and policies in respect of Personal Data protection;
   e. to conduct research and studies on technical standards for the protection of Personal Data, including international best practices with applicability to the Republic of Indonesia;
   f. to conduct research and studies and promote educational activities relating to Personal Data protection, including organizing and conducting seminars and workshops relating to such activities, and supporting other persons conducting such activities;
   g. to manage technical cooperation and exchange in the area of Personal Data protection with other persons, including foreign data protection authorities and international or inter-Governmental organizations;
   h. to consult with the private sector and consumer groups in relation to regulations and other measures that give effect to the objectives set out in this Law, including appropriate voluntary measures and self-regulatory frameworks where applicable;
   i. to conduct research and studies on ethical frameworks for the processing of Personal Data in connection with new technologies, including artificial intelligence;
   j. to represent the Government internationally on matters relating to personal data protection, including international cooperation as described in Chapter XI of this Law;
   k. to carry out functions conferred on the Personal Data Protection Commission under any other written law; and
   l. to develop the necessary capabilities to support the performance of these functions.