18 March 2019

His Excellency
Bapak Rudiantara
Minister of Communication and Information Technology, Republic of Indonesia
Jl. Medan Merdeka Barat No. 9, Jakarta

Cc.: Bpk. Semuel A. Pangerapan, Director General of Information Technology Application, Ministry of Communication and Information Technology, Republic of Indonesia

Subject: Industry Submission and Recommendations on Indonesia Personal Data Protection Draft Bill

Your Excellency,

On behalf of the Asia Internet Coalition ("**AIC**") and its members, I am writing to express our sincere gratitude to the Ministry of Communication and Information Technology, for the opportunity to submit comments on the Indonesia Personal Data Protection Draft Bill ("**Draft Bill**"). AIC is an industry association comprised of leading Internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of Internet and ICT policy issues. Our current members are AirBnB, Amazon, Apple, Expedia Group, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Oath), and Booking.com.

We commend the Ministry on formulating the Draft Bill that was disclosed to the public in February 2019. We also understand the government's intention to place regulatory frameworks to protect individual's personal data, especially those that are transmitted through the electronic system. We therefore support the government's intent in proposing this regulatory framework, but we do have significant concerns about the scope and impact of some of the provisions.

The summary of issues and concerns regarding provisions on the Draft Bill have been prepared based on our industry expertise and international best practices. As responsible stakeholders in this policy formulation process, we appreciate the ability to participate in this public consultation and submit our views. As such, please find appended to this letter detailed comments and recommendations, which we would like to respectfully request the Ministry to consider when reviewing the Draft Bill.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Importantly, we would also be happy 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 Personal Data Protection Bill.

Sincerely,

Jeff Paine
Managing Director,
Asia Internet Coalition

Enclosure

ASIA INTERNET COALITION

DETAILED COMMENTS AND RECOMMENDATIONS

From the given draft bill, we have identified three essential points that we strongly suggest revising in order to strengthen the draft quality and to meet global best practices:

1. **Potential extra-territorial effect**
   Chapter 1, Article 2 states that the law applies to every Person, Public Authority, Business, and organization/institution "both within the Indonesian jurisdiction and outside Indonesian jurisdiction, with legal consequences within the Indonesian jurisdiction and/or outside of Indonesian jurisdiction and harms the interest of Indonesia". This provision is extremely broad and seems to amount to Indonesia seeking to exercise extra-territorial effect on entities across the world, which would not be enforceable. Similar to other countries' personal data protection laws, we would propose that this provision be amended to ensure that organizations resident outside Indonesia are not caught by this law. The law should apply to the organizations that are formed or recognized under the laws of Indonesia or ordinarily resident. Please refer to Article.

2. **Unclear distribution of responsibilities between the parties involved**
   Chapter 1, Article 5 introduces the concept of the "Third Party." This creates an unnecessary level of confusion in the data lifecycle, which could result in a gap in protection of personal data or imposing impractical obligations on parties involved in the handling of personal data. The regulation should instead focus on clarifying the obligations of a data controller and data processor throughout the regulation. Meanwhile, in Chapter 6, Article 43 the mutatis mutandis responsibilities between data controller and processor is highly problematic. It blurs the obligations of a Data Controller and Data Processor without regard for their respective roles in the data lifecycle and differing visibility and degree of control over the decisions for collecting and processing personal data. This provision is in complete contrast to modern data protection laws that make a very clear distinction between the roles of a data controller and data processor such as the GDPR, and the Philippines Privacy Laws.

3. **Impractical data subject rights to implement**
   There are several rights of data subjects in Chapter 4, Article 18, 20, 21, 22, 25 that should be removed because they are already addressed through existing rights or are highly impractical to implement, without any corresponding data protection objective. The regulation should recognize a right of the Data Controller to charge a reasonable fee or refuse to act in relation to such Data Subject requests where the request would be unduly burdensome, manifestly unfounded or excessive. In line with other modern data privacy laws elsewhere in the world, the regulation should provide for flexibility in terms of legal bases for the collection and processing of personal data. Each basis should be treated as equally valid instead of creating complex exceptions. While the regulation recognizes some exceptions to consent these are not sufficiently robust to address modern business practices and the realities of data flows. The regulation should also recognize alternative methods of giving consent such as deemed consent and implied consent.

1. CHAPTER 1: GENERAL PROVISIONS

a. ***Article 1(5):*** *Third Party is any Person, Public Authority, and other body than Personal Data Subject, Personal Data Controller, Personal Data Processor, and other parties who, under the direct authority of the Personal Data Controller or Personal Data Processor, are authorized by Personal Data Controller or Personal Data Processor to process Personal Data.*

Recommendation: The concept of the "Third Party" creates an unnecessary level of confusion in the data lifecycle, and this could result in a gap in protection of personal data or imposing impractical obligations on parties involved in the handling of personal data. The regulation should instead focus on clarifying the obligations of a data controller and data processor throughout the regulation. We recommend deleting the concept of Third Party from the draft.

b. ***Articles 1(6), 1(10), 1(11), 24:*** *A Person is an individual, either Indonesian citizens, foreign nationals, or corporation. Corporation is an organized collection of persons and/or assets, both legal entities and non-legal entities. Business Actors are any individual or business entity, both in the form of legal entities and non-legal entities, established and domiciled or engaged in activities within the jurisdiction of the Republic of Indonesia, individually or jointly, through agreements to conduct business activities in various economic fields.*

***Recommendation*:** The concepts of "corporation", "Person", "Business Actor" and "organization" are overly complex. The regulation should instead distinguish between (i) natural persons and (ii) a unified concept of an "organization" (whether public or private, and whether or not legal entities).

We recommend removing the concept of corporation and replacing with "organization".
"*Organization" means any individual, company, association or body of persons, corporate or unincorporated, or public authority:*
... formed or recognized under the laws of Indonesia; or ordinarily resident

c. ***Article 2:*** *This Law applies to every Natural Person, Public Authority, Business, and organization/institution that carries out legal action as regulated in this Law, both within the Indonesian jurisdiction and outside Indonesian jurisdiction, with legal consequences within the Indonesian jurisdiction and/or outside of Indonesian jurisdiction and harms the interest of Indonesia.*

Recommendation: The scope of the Law should be limited to Indonesia and for the benefit of Indonesian data subjects. As such the Law should apply to Organizations established in Indonesia when they process personal data of Indonesian residents. We recommend replacing the Article Wording to: *"This Law applies to every natural person, and Organization that processes Personal Data relating to a Data Subject that is an Indonesian citizen or ordinarily resident in Indonesia".*

2. CHAPTER 4: RIGHTS OF PERSONAL DATA SUBJECT

a. ***Article 8, 14, 17:***

- *Personal Data Subject has the right to complete Personal Data prior to processing by Personal Data Controller.*
- *Personal Data Subject has the right to select or not selecting Personal Data processing through pseudonymization for certain purpose.*
- *Personal Data Subject has the right to delay or limit Personal Data processing proportionally in accordance with the purpose of the said Personal Data processing*

***Recommendation*:** There are several rights of data subjects that should be removed because they are already addressed through existing rights or are highly impractical to implement, without any corresponding data protection objective. These rights should be removed as they are already addressed in substance by other Data Subject rights in the regulation.

b. ***Article 18:*** *Implementation of the rights of Personal Data Subject as referred to in Article 9, Article 10, Article 11, Article 12, Article 13, and Article 15 are submitted through written request to the Personal Data Controller*

Recommendation: The regulation should recognize a right of the Data Controller to charge a reasonable fee or refuse to act in relation to such Data Subject requests where the request would be unduly burdensome, manifestly unfounded or excessive.

The following should be added to Article 18:

Where requests from a Data Subject are manifestly unfounded, unduly burdensome or excessive, in particular because of their repetitive character, the Data Controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
(b) refuse to act on the request. The Data controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request

c. **Article 20, 21, 22, 25:** *[Original articles are too long to be quoted]*

Recommendation: In line with other modern data privacy laws elsewhere in the world, the Regulation should provide for flexibility in terms of legal bases for the collection and processing of personal data. Each basis should be treated as equally valid instead of creating complex exceptions. While the regulation recognizes some exceptions to consent these are not sufficiently robust to address modern business practices and the realities of data flows. The regulation should also recognize alternative methods of giving consent such as deemed consent and implied consent.

The Information required to be given in Article 25(2) in order for a valid consent should focus on the purposes for the collection, use of disclosure of personal data. All other information to be provided (e.g. retention period) should be a separate obligation, and not a condition to a valid consent.

The regulation should incorporate additional grounds for lawfully processing personal data and also alternative forms of providing consent.

This provision will not apply to:

(a) opinion data kept solely for an evaluative purpose;
(b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;
(c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;
(d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;
(e) a document related to a prosecution if all proceedings related to the prosecution have not been completed;
(f) personal data necessary for the exercising of the right of freedom of expression and information, for compliance with a legal obligation, performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claim.

d. ***Article 25, 27:***

(4) In the event of Information change in Personal Data processing as referred to in paragraph (2), Personal Data Controller is required to notify Personal Data Subject no later than 7

(seven) days from the date of the Information change.

(2) Personal Data Controller is required to stop Personal Data processing as referred to in paragraph (1) no later than 3 (three) days from the request date for withdrawal of consent for Personal Data processing is received.

***Recommendation*:** The time period for notifications set out in Articles 25 and 27 are arbitrary and may not be practical in all the circumstances. Instead, these time frames should be changed to a "reasonable time" in light of the applicable circumstances. These time frames should be changed to a language of "reasonable time in light of the applicable circumstances".

e. Article 28:

(1) Personal Data Controllers must process Personal Data either partially or wholly in the event of request by Personal Data Subject.
(2) Delaying Personal Data processing as referred to in paragraph (1) exempted in the event of:
(a) there are laws and regulations that do not allow delays made by Personal Data Controllers;
(b) could harm the safety of others; and/or
(c) Personal Data Subject is bound to written agreement that does not allow delay of Personal Data processing.

Recommendation This provision is unclear, and it is not practical to implement. We recommend removing this provision.

f. Article 29 (a): *Personal Data Controller is required to protect and ensure the security of the Personal Data it processes, by doing: preparation and application of operational technical steps to protect Personal Data from disruption of Personal Data processing that is contrary to the provisions of the legislation; and*

***Recommendation*:** It is unclear what it means to protect Personal Data from disruption of Personal Data processing. Personal Data Controller is required to protect and ensure the security of the Personal Data in its possession or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.

3. CHAPTER 4: RESPONSIBILITIES OF DATA CONTROLLER, DATA PROCESSOR, AND THIRD PARTY IN PROCESSING DATA

a. Article 33: *Each Personal Data Controller and Personal Data Processor must record all activities of Personal Data processing.*

***Recommendation*:** This obligation is overly broad and could impose an undue burden that is costly and impractical on all parties operating in Indonesia, without a clear data protection outcome. The obligation to maintain records should be primarily on the data controller who has visibility into the purpose for which the personal data is collected and processed. The data processor often will not have knowledge of the purpose. Moreover, this requirement should be limited to specific categories of information that have a clear link to a data protection outcome for example, the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; where applicable the categories of recipients to whom the personal data may be disclosed.

There should also be an exemption for small / medium enterprises for whom such a requirement would pose an economically infeasible obligation. This is recognized in the GDPR, which provides an exemption for organizations with fewer than 250 employees.

Each Data Controller shall maintain records that sufficiently describe its data processing system, and

identify the duties and responsibilities of those individuals who will have access to personal data. Records should include:

(a) Information about the purpose of the processing of personal data, including any intended future processing or data sharing;
(b) A description of the general categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing;

General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data.

b. Article 34:

(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.
(2) The granting of access to Personal Data Subject as referred to in paragraph (1) is carried out from the date of receipt of the application for access in accordance with the period of Personal Data retention.

Recommendation: It is impractical for Data Controllers to produce potentially lengthy records on the request of a data subject, and may require the exposure of corporate confidential information such as security practices. It also does not seem to serve any particular data protection objective as this right can be addressed through one of the other rights of data subjects e.g. right to access and correct. We recommend removing this requirement.

c. Article 36:

(1) Personal Data Controller is required to fix error and/or inaccuracy of Personal Data immediately after receiving request of Personal Data revision from Personal Data Subject.

***Recommendation*:** The time frame provided for correction of personal data is impractical and out of step with international practice.

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. This provision will not apply to:

(a) opinion data kept solely for an evaluative purpose;
(b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;
(c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;
(d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;
(e) a document related to a prosecution if all proceedings related to the prosecution have not been completed;
(f) personal data necessary for the exercising of the right of freedom of expression and information, for compliance with a legal obligation, performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claim.

d. Article 40(1)

Personal Data Controllers must erase Personal Data processing in the event of:
(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 through written request to the Personal Data Controller; and/or*
(c) *Personal Data is obtained and processed in an illegal manner.*

***Recommendation*:** Obligation to erase Personal Data subject to a condition that retention is no longer necessary for legal or business purposes. Replace the Article Wording to: *Personal Data Controllers must erase Personal Data processing in the event of: Personal Data is no longer needed to achieve the purpose of Personal Data processing and retention is no longer necessary for legal or business purposes.*

e. ***Article 40(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.*

***Recommendation*:** This provision is confusing, and it is unclear what data protection objective it is intended to serve. We recommend deleting this provision.

f. **Article 42**

1. *In the event of failure to protect Personal Data, the Personal Data Controller must submit a written notice within no later than 72 (seventy-two) hours to:*
    a. *Personal Data Subject; and*
    b. *Minister or Sector Supervisors and Regulatory Agency in accordance with the provisions of legislation;*
2. *In the event of Sector Supervisory and Regulatory Agencies receive notification as referred to in paragraph (1), Sector Supervisory and Regulatory Agencies can coordinate with the Minister.*
3. *Notification in writing as referred to in paragraph (1) regarding:*
    a. *Personal Data disclosure:*
    b. *when and how Personal Data is revealed; and*
    c. *efforts to handle and recover the disclosure of Personal Data by Personal Data Controllers.*
4. *In certain issues the Personal Data controller is obliged to notify the community regarding the failure of Personal Data Protection as referred to in paragraph (1).*

***Recommendation*:** All access to information and facilities under the Law should be subject to checks and balances and judicial oversight to ensure that rights of individuals and private actors are protected and the potential for abuse of power is limited. Any access to information or facilities should be required with a valid court order. There should also be rights for data controller to dispute or contest the order, command, or request.

Orders, commands or requests should be limited to situations where there is a significant risk of serious harm, and such harm should be balanced against other criteria, such as impact on the community, commercial and other practical impacts.

The Law should include clearer obligations on the relevant regulator to maintain the confidentiality of information provided to them and to protect the information from unauthorized disclosure / use and to securely dispose of the information after their investigation is completed or the information is no longer required by the regulator for its legitimate supervisory purposes.

This provision should be revised altogether to be in line with international practices on data breach notification regimes.

g. ***Article 43:*** *In the event Personal Data Processor is appointed by Personal Data Controller, all provision for Personal Data Processing applies mutatis mutandis to Personal Data Processors.*

***Recommendation*:** This requirement is highly problematic as it blurs the obligations of a Data Controller and Data Processor without regard for their respective roles in the data lifecycle and differing visibility and degree of control over the decisions for collecting and processing personal data. This provision is in complete contrast to modern data protection laws that make a very clear distinction between the roles of a data controller and data processor such as the GDPR, and the Philippines Privacy Laws. In line with these privacy regimes, this provision should require the data processor to comply with the lawful instructions of the data controller.

The Data Processor and any person acting under the authority of the Data Controller or of the Data Processor, who has access to personal data, shall not process those data except on instructions from the Data Controller, unless required to do so by a law of Indonesia.

h. ***Article 44(4):*** *In the event of Personal Data Processor as referred to in paragraph (3) carried out Personal Data processing outside the purposes specified by Personal Data Controller, then it is entirely the responsibility of the Personal Data Processor concerned.*

Recommendation: As with the comments on Article 43, this requirement imposes impractical obligations on the data processor. The data processor should be responsible for complying with the lawful instructions of the Data Controller and be responsible for the harm suffered by the data subject if they act outside of such instructions. However, the Data Processor cannot have the same responsibilities as a Data Controller as this would be impractical, and in some cases potentially impossible to implement. We recommend removing this provision.

i. ***Article 45:*** *Third Party is required to process Personal Data in accordance with Personal Data Processing purposes consented by Personal Data Subject.*

Recommendation: The introduction of a third party in this provision creates uncertainty in the data processing chain and it should be removed. We recommend removing this provision.

4. CHAPTER 7: DATA TRANSFERS

a. ***Article 49(1):*** *Personal Data Controllers or Personal Data Processors can transfer Personal Data to Third Parties within the territory of the Republic of Indonesia.*

b. ***Article 49(2):*** *Personal Data Controller or Personal Data Processor who transfers and the third party receiving the Personal Data transfer as referred to in paragraph (1) are obliged to carry out Personal Data protection as referred to in this Law.*

c. ***Article 50:*** *Personal Data Controller must request and obtain written consent from Personal Data Subject prior to transferring the Personal Data they process to any third party outside the jurisdictional territory of the Republic of Indonesia.*

d. ***Article 50:*** *Personal data as referred to in Article 50 may be transferred outside the jurisdiction of the Republic of Indonesia provided that:*

- *i. the country or international organization has a level of Personal Data protection which is equal to or higher than this Law,*
- *ii. there is a contract between Personal Data Controller and a third party outside the territory of the Republic of Indonesia by taking into account the aspects of Personal Data protection; and/or there is an international agreement between countries*

Recommendation: The current drafting of the data transfer regime is unusually complicated with provisions for (a) general transfers of personal data to other parties under Article 53, (b) transfers within Indonesia and (c) transfers outside of Indonesia. It is unclear for example why there should be separate provisions for transfers to third parties generally at all. The Data Controller should be responsible for the transfer of personal data to third parties whether within Indonesia or outside of Indonesia. This is because the Data Controller typically is the party that knows the purposes for which the personal data has been collected and has the direct relationship with the data subject to provide relevant notifications / obtain relevant consents from them. The regulation should provide for several

standalone bases on which transfers of personal data outside of Indonesia are permitted. This would bring the regulation in line with GDPR as well as other regional privacy laws such as in the Philippines, Singapore, and Malaysia.

The Personal Data Controller is responsible for any personal data under its control or custody, including information that have been outsourced or transferred to a Personal Data Processor or a third party for processing, whether domestically or internationally.

A Personal Data Controller may transfer Personal Data outside the jurisdiction of the Republic of Indonesia if:

(a) It is satisfied that the country to which the Personal Data will be transferred provides an comparable or higher level of personal data protection as this Law;
(b) There is a contract between the Personal Data Controller and the recipient of the personal data;
(c) There is an international agreement between the countries;
(d) The Data Subject has consented to the transfer;
(e) The Data Controller has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available
(f) There are applicable binding corporate rules regarding personal data protection between members of a corporate group
(g) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(h) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(i) the transfer is necessary for important reasons of public interest;
(j) the transfer is necessary for the establishment, exercise or defence of legal claims;
(k) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

e. ***Article 45:*** *Personal Data Controller, Personal Data Processor and/or Third Party are prohibited to disclose specified Personal Data to other party.*

Recommendation: This should be deleted in line with the above and we recommend removing this provision.

5. CHAPTER 8: PROHIBITION

a. ***Article 56:*** *Third Party is prohibited from Personal Data processing for other than Personal Data Processing purposes consented by Personal Data Subject.*

Recommendation: This provision is contradictory and overlaps with the general provisions regarding data subject rights, including the right to consent. This provision unnecessarily introduces complexity into the parties involved in the data lifecycle and should be deleted. We recommend removing this provision.

b. ***Article 57:*** *Personal Data Controller is prohibited to transfer Personal Data they process out from the jurisdictional territory of the Republic of Indonesia without the consent of Personal Data Subject and violate the following regulation:*

i. the country or international organization has a level of Personal Data protection which is equal to or higher than this Law;
ii. there is a contract between Personal Data Controller and a third party outside the territory of the Republic of Indonesia by taking into account the aspects of Personal Data protection; and/or

iii. *there is an international agreement between countries.*

Recommendation: This provision appears to create an overlapping / repetitive requirement and should be deleted. Please refer to comments on Articles 49-51. We recommend removing this provision

c. ***Article 58:*** *Personal Data Controller and Personal Data Processor are prohibited to process Personal Data for commercial and/or profiling purposes unless there is consent from the Personal Data Subject.*

Recommendation**:** This obligation should only apply to the Personal Data Controller. The Data Processor typically has no visibility into the purposes for which the personal data has been collected or the scope of the consents provided. Moreover, the Personal Data Processor does not typically have a direct relationship with the Data Subject to be able to practically obtain consents. "Commercial" purposes is also far too broad and it is unclear what this is intended to protect. A clear definition of profiling should also be included.

Replace the Article Wording to: *Personal Data Controller are prohibited to process Personal Data for profiling purposes unless: (a) there is consent from the Personal Data Subject; (b) such processing is necessary for entering into, or performance of, a contract between the data subject and a data controller; or (c) it is permitted under a Law of Indonesia.*

Further explanation:
'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

The exemptions should be expanded to include: (a) anonymized data + pseudonymised data, (b) data processed for historical purposes, (c) Personal data processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations, (d) processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity.

6. CHAPTER 14: CRIMINAL PROVISIONS

a. ***Article 71:*** *Third party who intentionally and unlawfully processes Personal Data other than for the purpose consented by Personal Data subject as referred to in Article 56 is liable to a fine of a not more than Rp500.000.000- (five hundred million rupiah).*

Recommendation**:** This provision conflates the role of the Data Controller and Data Processor and creates an inappropriate liability regime. Moreover, it does not recognize other legal bases for the processing of personal data as set out in the regulation and therefore creates confusion. The Data Processor will typically have no visibility into the purposes for which personal data has been collected or the processing decisions that the Data Controller makes with respect to that Personal Data.

b. ***Article 72:***

Personal Data Controller who deliberately transfer Personal Data out from the jurisdictional territory of the Republic of Indonesia without consent of Personal Data Subject and violate the following regulation:

(a) the country or international organization has a level of Personal Data protection which is equal to or higher than this Law;
(b) there is a contract between Personal Data Controller and a third party outside the territory of the Republic of Indonesia by taking into account the aspects of Personal Data protection; or

(c) there is an international agreement between countries, as referred to in Article 57, is liable to a fine of a not more than Rp50,000,000,000. - (fifty billion rupiah).

***Recommendation*:** As explained in Article 56 above, this creates an overlapping requirement for data transfers. There should be a single regime in the regulation for data transfers to ensure that all parties have a clear understanding of the appropriate bases on which personal data may be transferred offshore.

c. ***Article 71:*** *Any person who intentionally disclose or use Personal Data that does not belong to them without consent of the Personal Data Subject as referred to in Article 59 is liable to a fine of a not more than Rp10,000,000,000. - (ten billion rupiah).*

***Recommendation*:** This provision contradicts other sections of the regulation that allow for use or disclosure of personal data without consent. The wording of the article should be replaced with: *"Any person who intentionally discloses or uses Personal Data that does not belong to them in contravention to this Act is liable to a fine of a not more than Rp10,000,000,000. - (ten billion rupiah)".*

- ***End of Submission***