Asia Internet Coalition (AIC) Industry Response to Draft Implementation Regulation of Indonesian Law No. 27 of 2022 concerning the Protection of Personal Data

25 September 2023

To
Mr. Budi Arie Setiadi,
Minister of Communication and Information Technology (KOMINFO)
Jl.Medan Merdeka Barat
No.9 Jakarta Pusat,
10110 Jakarta, Indonesia

Dear Minister Budi Arie Setiadi,

The Asia Internet Coalition (AIC) would like to express our sincere gratitude to the Ministry of Communication and Information Technology (KOMINFO) for the opportunity to submit comments on the Draft Implementation Regulation of Indonesian Law No. 27 of 2022 concerning the Protection of Personal Data (Draft Implementing Regulation).

As an introduction, the Asia Internet Coalition (AIC) is an industry association comprising leading internet and technology companies. We seek to promote technology and policy issues in the Asian region, and we are fully committed to the cause of a safe and open internet.

First and foremost, we commend the Government of Indonesia and KOMINFO's intent to align Indonesian law with global and local demands for increased transparency on how service providers utilize personal data. We endorse the promotion of ethical and responsible innovation in personal data usage.

We also share KOMINFO's belief that consumers should be able to engage in transactions with confidence in the protection of their personal data. Nevertheless, we believe that businesses should not be burdened with excessive requirements that do not significantly enhance consumer data protection.

On this note, we wish to highlight that the Draft Implementing Regulation includes provisions that (i) impose cumbersome record-keeping and auditing obligations on both personal data controllers and processors without substantially improving consumer data protection, (ii) place requirements on personal data processors who lack control or direct interaction with the personal data they process under the direction of controllers or data subjects, and (iii) subject personal data processors to multiple and repetitive penalties.

We are concerned that the Draft Implementing Regulation, in its current form, may impact many personal data processors and may lead them to limit their services in Indonesia. This can potentially result in unintended negative consequences for consumer choice in Indonesia and its digital economy.

As responsible stakeholders in this policy formulation process, we would greatly appreciate the opportunity to share – **in the Sections below** - our key recommendations and detailed comments on the Draft Implementing Regulation which we would like to respectfully request KOMINFO to consider when finalizing the draft regulation.

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. Furthermore, we would also be happy to offer our inputs and insights on industry best practices, directly through discussions and help shape the dialogue for the advancement of Indonesia's digital economy.

Thank you
Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Detailed Comments and Recommendations

Section A: Overview of Key Recommendations

1. **Arts. 21, 137, 156, 157, 158 and 159: We recommend a clearer distinction between the responsibilities of personal data controllers and personal data processors**. Personal data processors do not have the same relationship with data subjects and typically are not in a position to make meaningful or independent decisions about the processing of personal data – rather they implement decisions of a data controller. It is therefore inappropriate for personal data processors to be held accountable to data subjects. In the cloud computing context, for example, personal data processors - being the cloud services provider - often have no visibility on the data being processed by them (and are unable to distinguish personal data from other types of data). It would

therefore be inappropriate for them to have the same or similar obligations as a personal data controller, such as the obligation to ensure the accuracy, completeness and consistency of the personal data; to determine the appropriate level of security to protect the personal data; and to maintain confidentiality of the personal data. The law should make clear that the rights and obligations relating to 'access, storage, security, disclosure, deletion, security breach notification etc.' (various stages of handling of data) should remain with the personal data controller. Alternatively, we recommend the Draft Implementing Regulation to clarify that that the above mentioned Articles apply to personal data processors only to the extent that the specified obligations fall within the personal data controller's instructions to the personal data processor so that it does not conflict with Art 155(1).

2. **Arts. 87, 157, 192: We recommend removing prescriptive obligations that increase record-keeping and compliance burdens while not necessarily increasing protection for personal data.** Data protection laws should avoid imposing requirements that generate unnecessary administrative burdens on organizations, without providing additional protections for the data subject. Such requirements include providing a record of processing in the event requested by the PDP Institution (Art 87(8)), and conducting or keeping record of impact assessments without considering the scope, context, sensitivity and purposes of the processing. Such requirements do not offer an additional level of protection to personal data, and instead divert valuable PDP Institution (PDPI) resources from the investigation and enforcement of serious breaches, to creating complicated and costly administrative processes. It also reduces the ease of doing business, especially if the record-keeping requirements result in bottlenecks. Unlike many other regulated areas – PDP regulations have broad and wide applicability, as they tend to apply to all organizations that process personal data. Therefore, such compliance burdens are likely to impact a majority of businesses in Indonesia.

3. **Arts 21, 32(3), 137: We recommend removing prescriptive requirements from the scope of the agreement between personal data controllers and personal data processors ("Data Protection Agreement"), including the requirement for the Data Protection Agreement to be in Bahasa Indonesian language**. This approach (including the local language requirement) is unprecedented in ASEAN and even the Asia Pacific countries, overly-specific and is not aligned with international data protection frameworks. We caution against prescriptive and mandatory requirements in the Data Protection Agreement as they present a significant operational burden for organizations that operate across multiple countries and often use a single agreement that applies across multiple jurisdictions and complies with the standards of those jurisdictions. We recommend instead that KOMINFO provide principles-based guidelines based on international standards so that organizations have the flexibility to determine the content of the Data Protection Agreement that accurately reflect the responsibilities of the personal data controller and the personal data processor in the processing of personal data.

4. **Art 187: We recommend that any standard contractual clauses that will be determined in a subsequent regulation by the PDPI should align with the equivalent standard contractual clauses under the European Union's General Data Protection Regulation (GDPR)**. **We also recommend removing the obligation to conduct due diligence on other third parties to whom personal data is transferred**

(Art 187(2)(d)) and the wide discretion for personal data controllers to add new standard contractual clauses in accordance with their needs (Art 187(3)) as part of the scope of the standard contractual clauses as it is not in line with internationally recognised standards. This is important not only to ensure an equivalent standard of privacy protection for personal data transferred overseas, but also to promote harmonized international standards, reduce the compliance burden on global organizations which have already updated their contractual clauses to comply with GDPR requirements, and avoid confusion for organizations and individuals. In addition to ensuring an equivalent standard of data protection for personal data transferred overseas, harmonizing Indonesia's data protection regime with international standards helps boost Indonesia's competitiveness as a business destination. Further, we strongly recommend KOMINFO to carry out thorough and robust consultation with all relevant stakeholders prior to the formulation of the standard contractual clauses. This will ensure that the standard contractual clauses will be technically feasible and cognizant of the interests of all stakeholders.

5. **Arts 192, 194, 195: We recommend removing cross-border data transfer obligations that are inappropriately imposed on personal data processors.** For example, the obligations to record data transfers and ensure that data transferred is sufficient, relevant and limited (Art 192), and to provide a notification with prescribed information about the data transfer to the data subject (Art 195) should be placed solely on personal data controllers that control and determine the purposes and means of processing personal data, including its transfer overseas. We also recommend removing the obligation on personal data controllers and/or personal data processors to carry out a data transfer impact assessment (Art 194). In practice, it will result in additional administrative burden and operating costs for organizations. It will also be resource-intensive for government authorities to manage and review an enormous number of administrative processes in the form of impact assessments.

6. **Arts 27, 28, 30, 32, 101, 126, 134, 135, 139**: **We recommend removing prescriptive internal obligations and policy requirements that are imposed on the data controller**. While we acknowledge the necessity to have internal policies, an overly prescriptive approach to what these policies should include is unlikely to be practicable for international companies that operate on a global basis. We recommend consistency with international data privacy standards where organizations have the discretion to set proportionate measures that meet the needs of the data subjects, in line with data protection principles such as accountability.

7. **Art 166: We recommend removing this Article which requires the personal data controller and/or personal data processor to appoint a personal data protection officer (DPO) taking into account the structure, size and organizational needs of the personal data controller and/or personal data processor.** Such requirement increases the cost of operations for organizations, does not offer an additional level of protection to personal data and reduces the ease of doing business in Indonesia.

8. **Arts. 115-120: We recommend (a) clarifying that Part Fourteenth of the Draft Implementing Regulations do not subject data controllers and processors to joint**

and several liability, and (b) removing the requirement for personal data controllers to maintain a procedure and policy for addressing direct compensation requests from personal data subjects. While Art 115 states that this right is based on the fault or negligence of the controller, the subsequent Articles places joint and several liability on personal data processors to provide compensation. First, we do not support joint and several liability regimes as they undermine data protection outcomes by (a) creating a moral hazard where one party is incentivized to neglect its obligations because the other party will be jointly liable; and (b) unfairly prejudicing an innocent party for another's breach. For example, smaller businesses that are data controllers may neglect their data protection obligations if they know that data subjects are more likely to seek compensation from a more visible data processor (such as an online platform or cloud service provider), even if the processor had not breached its own obligations under law. Second, we do not recommend giving personal data subjects the statutory right to demand compensation from data controllers or processors for violations of personal data protection regulations. Requiring companies to maintain a process and policy to address compensation requests is administratively burdensome. Rather, such disputes should be adjudicated in court and according to due process and the rule of law. To the extent KOMINFO's aim is to encourage out-of-court settlements for breaches of data protection regulations, this option is generally available to parties even without a statutory right.

9. **Art. 49. We recommend that service providers should not be forced to provide services to consumers if those consumers refuse to consent to data processing.** The draft PDP Regulations contain a prohibition to refuse providing services where the data subject does not consent. We recommend that service providers should not be forced to provide services to consumers if those consumers refuse to consent to data processing. As currently drafted, Art. 49 provides that entities cannot refuse to provide a service, or provide a worse service, if a consumer refuses to provide consent to data processing. This is extremely challenging for all data controllers and leads to the absurd result that companies are required by the PDP Law to provide a service, but may breach the PDP Law in doing so because they do not have consent for data processing.

10. **Arts. 13, 28, 82, 85, and 156: Clarify that verification requirements are limited to correcting information where the controller is made aware that it is inaccurate:** Throughout the draft PDP Regulations, there are vague requirements to conduct 'verification' to ensure accuracy, completeness and consistency (see, for example, Articles 13, 28, 85 and 156). In Article 82, it is specifically required that controllers verify the "level of truth and / or trustworthiness" of personal data. This type of proactive requirement to verify truthfulness is unworkable. We recommend that references to verification be clarified to make it clear that the requirements are limited to correcting information where the controller is made aware that it is inaccurate.

11. **(Various Articles, including Article 70) Providing Reasonable Limitations on Data subject rights, including the right to object :** Data subject rights under the draft PDP Regulations do not contain sufficient exceptions to be workable. The framing of data subjects rights is also drafted in an extremely broad manner which implies that requests must be honored *whenever* they are made, instead of where specific conditions are met (see, for example, Articles 93(1)(c), Article 95(1)(c) and Article 97(1)(b)). The right to

object to processing under Article 70 should be limited. Under the GDPR, the right to object is not absolute and data controllers can reject the objection request if it "demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims." These same exceptions should be built into the PDP Regulations.

12. **(Arts. 55 (1), 57, and 70). Ensuring consistency with Global Best Practices on the Legal Bases for Processing Data.** The PDP Regulations introduce limitations on when contractual necessity and legitimate interests can be relied on to process personal data which are out of step with global data protection law norms. This will make it more challenging for data controllers to rely on these legal bases, pushing them towards an undue over-reliance on consent, which will have negative impacts on businesses and consumers, such as notice fatigue. We recommend that Articles 55(1) and Article 57 be deleted, as they are confusing, unworkable, and contain a long list of unnecessary requirements for agreements which are used as the basis for processing personal data, which is not seen in any other privacy laws globally. We additionally recommend that Article 70 be redrafted in a manner consistent with GDPR norms regarding the use of legitimate interests as a legal basis for processing data.

Section B: Article Wise Comments

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
1	Article 1 Child means any person under the age of 18 (eighteen) years old and unmarried.	Most laws define the age of a child between 13-16 years. For example, under the GDPR, the age at which a child can consent to the processing of their personal data is 16 years old. It is important to give a gradient of online experiences as teenagers have differing needs and cognitive abilities than young children (eg under 13). The Internet and digital technologies are critical for teenage development, learning, access to information and community, and should be leveraged in safe, age appropriate ways rather than restricted for older teens. We suggest the definition of a child be set between 13-16 to align with international best practices.

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
2	Article 7(1) on categories of Specific Personal Data	We do not recommend including "child data" and "personal financial data" in the category for "specific" personal data. The inclusion of these data categories places a disproportionate compliance burden on companies. Child data: The fact that data relates to a child does not render it any more sensitive that would require a higher compliance requirement. Instead, the key risk arising from processing child data relates to whether the child is capable of providing informed consent. This has been addressed separately in the Draft Implementing Regulation by the requirement of parental consent. Requiring companies to have a higher compliance burden for "child data" is onerous where such companies provide products and services which are not necessarily directed at children and/or are only designed to be used with parental control. Such companies may not have the means to assess whether the user may have been a child using the parent's account. Personal financial data: The inclusion of "personal financial data" as a category of "specific" personal data is inappropriate where such data may be processed in the ordinary course of e-commerce transactions. For example, it is normal to process "personal financial data" about individuals when processing payments or reviewing applications from customers who want to use monthly billing systems, etc.
3	Article 10 (2) "Objection on automatic processing"	Article 105 (2) "Actions which have legal consequences or significant impacts to Personal Data Subject" is defined too broadly and therefore a service provider may be burdened to accommodate endless possibilities.

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
4	Article 12 The Draft PDP Regulation still provides a broad scope on 'other specific personal data', without setting out what these types of data are and only providing general factors (in Article 7(2)). It further grants a minister or institution to determine 'other specific personal data' after coordinating with the data protection agency.	We recommend that the guidelines be more specific in setting out what other specific personal data covers. Further, we seek clarification on how the minister or institution is able to influence the DPA authority to add 'other specific personal data', i.e., whether such determination of any new 'specific personal data' must be conducted under a law or other lower hierarchy of regulation.
5	Article 12 (2) “Procedures on imposing compensation due to PDP violation”	• Article 117: there is a conflict between point a which stipulates when filing compensation request, the Personal Data Subject does not have to provide any evidence of damages suffered and point b which stipulates otherwise. • Overall, there is no clarity on whether the compensation may be requested simultaneously by a Personal Data Subject to a Personal Data Controller in question, while he/she is filing a lawsuit to a court, and submitting a request to the PDP Authority Agency (even during or after a lawsuit has been filed to a court).
6	Article 13 (3) “Rights of personal data subject to use and send his/her personal data”	n/a

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
7	Article 16 (3) "Provisions on implementation of personal data processing"	• Article 49 (1) may create confusion when a Personal Data Controller, whose activities is based on or revolve around processing personal data, is being denied processing the personal data but is still required to provide its products and/or services to the Personal Data Subject. The "Personal Data Controller" in this article should be revised to a "product/service provider" in general. • Article 51 (4) may create a KYC level of verification process equals with the ones in the financial service industry which may create unnecessary complexity for business players in different industries. • Article 1 (21) about the definition of a "Child" is not aligned with other existing laws in Indonesia which have their own definition of "Child" and they are higher in regulatory hierarchy if compared to this draft government regulation.
8	Article 21 on: - agreements between a Personal Data Controller and Personal Data Processor - Personal Data Controllers comply to the 3 x 24 hours (72 hours) timeframe requirement	We do not recommend dictating terms / clauses that must be included in the contracts between controllers and processors. The nature of the relationship between such organizations could vary considerably and a set of inflexible standards could lead to inappropriate or impossible obligations being placed on these organizations in the context and nature of their relationship. Additionally, we do not recommend requirements for mandatory internal or external audits. Audit requirements are not appropriate or necessary in most circumstances, increasing the cost of compliance significantly without providing greater privacy protection for the data subjects. For example, SMEs and charitable organizations are unlikely to have the requisite budget to perform external audits, and making such audits mandatory could unnecessarily increase compliance costs for regulated organizations.

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		External audits also introduce security risks and potential disruptions to services offered by regulated organizations. These include the risk of service disruption and the corresponding liability for loss and damage to that entity's customers, if for example, the audit process inadvertently results in unauthorized disclosure or loss of personal data. We also do not recommend the appointment of a jointly appointed contact person as it is unclear how their responsibilities differ from a DPO, and is unnecessary duplicative. We suggest that the guidelines clarify that the agreement appointing a data processor may be made in a standalone agreement or incorporated into other agreements between the data controller and data processor. We seek further clarification on what needs to be fulfilled within the timeframe - providing notification or implementing requested action. We suggest there can be reasonable extensions of the 72-hour deadline in cases where compliance is genuinely challenging due to the volume or complexity of requests. This extension could be subject to specific criteria or requirements, ensuring that data controllers have valid reasons for needing additional time.

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
9	Article 24 on the principles of processing of personal data	We note that the option to 'anonymize' data in place, such that a person is no longer identifiable and the data no longer purports to be 'personal data' has been omitted from the Draft Implementing Regulation. We note that the inclusion of this option is especially important as it allows for the data to be retained for other business purposes but does not prejudice the rights of data subjects. We recommend that references to data deletion in the Draft Implementing Regulation also includes data anonymization as shown by reference to Art. 24.
10	Articles. 27, 28, 30, 32, 101, 126, 134, 135, 139 on internal obligations regarding internal policies on the data controller	We note that the obligations to develop internal policies as set out in the Draft Implementing Regulation exceed those set out in international data privacy standards. While we acknowledge the importance of internal policies, an overly prescriptive approach to what these policies should include, etc. is unlikely to be practicable for international companies that operate on a global basis. For example, the Draft Implementing Regulation imposes obligations on the controller to: ● "develop internal policies, procedures and/or guidelines" regarding certain issues e.g., to manage data subject rights requests, data accuracy, handling data breaches, audits, etc.; ● adopt and implement a general personal data protection policy and retention policy document; and

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		• establish internal policies for specific business units. However, comparable international standards reference such obligations on data controllers with respect to the underlying data protection principles (e.g., accountability) to allow companies to set proportionate measures that meet both the needs of the data subjects and the companies' internal operational requirements.
11	Articles 28, 32, 87 and 192 on record keeping obligations for the data controllers	The record keeping obligations set out in the Draft Implementing Regulation exceed those set out in international data privacy standards and are likely to impose an undue burden on international companies. For example, while international data privacy standards similarly require record keeping for processing activities, we note that Arts. 32 and 87 require record keeping for 'all' personal data processing activities, rather than those activities with significant impact on the data subject. Further, Arts. 28 and 87 require a record of the 'source of collection' of personal data and Arts. 87 and 192 require the mapping of personal data flows and the transfer cycles of personal data. We recommend that the requirements for data controllers are not so prescriptive that companies must dedicate significant resources to the data recording, which does not result in added protection for data subjects and even contradicts

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		other requirements for data controllers as set out in the Draft Implementing Regulation (e.g., data minimization, data retention, etc.)
12	Article 34 (3) "Provisions on impact assessment on personal data protection"	n/a
13	Article 47 With regard to withdrawal of consent through the mechanism provided. It's unclear on which mechanism is referred to here.	We seek further clarification on whether there could be separate mechanisms for obtaining and withdrawing consent, so long as these are effective.
14	Articles 48-49 on explicit and valid consent	We understand that the intention behind these Articles is that the data controller not carry out processing of personal data which is contrary to the Draft Implementing Regulation. However, it is unclear how these provisions work with Art. 44. For example, Art. 48(1) could be misinterpreted as requiring data controllers to cease processing if the data subject refuses consent, even if other legal bases may apply.

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		Additionally, we recommend including the fairness principle in Art. 48(2). Processing data in a way that is merely "discriminatory" is appropriate for different categories of data subjects. For example, businesses do treat customers, employees, business contacts, etc. differently depending on the circumstances. The problem is where that discrimination is unfair. For example, a company may apply much greater due diligence to hiring a senior manager than an intern; this does not necessarily mean that the senior manager candidate has been unfairly retreated. We recommend that Art. 49(1) clarify that the provision of goods or services may be refused where the consent to processing personal data is necessary (or possibly just reasonable) to provide such goods or services. For example, a company may not be able to provide customers with a free trial through their mobile carrier unless they consent to receiving such offers through their mobile carrier. It would be impracticable (and unfair to customers) for the company to be forced to make such offers even where the customer does not consent to receiving such offers. We further recommend that service providers should not be forced to provide services to consumers if those consumers refuse to consent to data processing. As currently drafted, Art. 49 provides that entities cannot refuse to provide a service or provide a worse service if a consumer refuses to provide consent to data processing. This is extremely challenging for all data controllers and leads to the absurd result that companies are required by the PDP Law to provide a service, but may breach the PDP Law in doing so because they do not have consent for data processing

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
15	Article 49 (1), (2), (3) The guidelines require data controllers to provide goods, services or assistance to data subjects who refuse to give consent. Although subparagraph (3) clarifies that such provision of goods, services and assistance is carried out as long as it does not require the processing of personal data, subparagraph (2) requires that there should be no effect on quality. This provision does not seem to be supported by any provision in the PDP law.	We recommend deleting 49(1), (2) and (3).
16	Article 48 (5) "Provisions on notification on merger, acquisition, dissolution"	n/a
17	Article 51 on parental consent (and Art. 1(21) on definition of child)	We recommend lowering the age limit under the Draft Implementing Regulation to align further with international standards for companies which operate on an international basis. The age of consent under the GDPR is 16 years of age but individual countries are permitted to lower the age of consent to 13 years old. This is more reflective of the way minors use technology today. Furthermore, international privacy standards only require parental consent when an online service is offered directly to children. This is an appropriate and proportionate measure to avoid an undue burden for services which are not directed at children. We recommend that the obligation for parental consent only apply if: (i) the controller

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		knows (actual or constructive knowledge) that the data subject is a child; and (ii) the services are directed to children (or likely to be accessed by children). We also seek clarification on the verification process for the consent from a child's parents / guardians (e.g. would a statement be sufficient).
18	Articles 52 and 53 on identification of users of the service	We recommend removing Arts. 52 and 53 as it is not clear what these mean and to what extent the measures need to apply. These obligations appear to require data controllers to verify users' identities even where it is not necessary or proportionate given the purpose of the processing. Additionally, such verification can be unnecessarily intrusive for the data subject when, for example, their disability may not be relevant to their use of the services/products. These duties also run counter to basic data minimization norms in those frameworks, by requiring additional, potentially unnecessary data, to be collected.
19	Articles 54-58 on fulfillment of agreement obligations / consent	We understand that KOMINFO wishes to encourage transparency where personal data controllers seek to obtain the consent of personal data subjects for the purpose of processing. However, a contractual agreement to document this may create more burden on both the controller and data subject. Art. 54 sets out the circumstances in which the contractual necessity legal basis is applicable, but does not include processing taken at the request of the data subject prior to entering into an agreement. This should be included to allow for pre-contractual data processing (e.g., know-your-customer checks, vendor due diligence, etc.). This will also ensure internal consistency with Art. 56(1)(b), which indicates pre-contractual processing is intended to be covered.

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		Additionally, Art. 57 provides a list of elements which must be included in the agreement, which adds on to the burden of the data subject who must now review the contract terms and decide whether or not to agree. Instead, we recommend that KOMINFO takes an approach similar to Singapore, and deem that consent is valid where the data subject has been notified of the purposes for which their personal data is collected, used, and disclosed, and he has provided consent for those purposes. We believe this strikes a balance between helping data subjects understand how their personal data will be processed on the one hand, and on the other, minimizing administrative burden on both data subjects and controllers. However, if KOMINFO chooses to retain Arts. 54-58, Art. 57 should be scoped down to prevent further consent or notification fatigue.
20	Article 54 (3) "Provisions on PDP officer"	Article 165 (1).b, it is not clear on what is considered with "big scale".
21	Article 54(5), (6) The articles make the basis of lawful agreement unclear (and inferior to "consent"). The rest of Article 54 and Articles 55 to 58 already provide enough safeguards and protections for the use of lawful agreement as basis for processing.	We suggest that Article 54(5) and (6) be deleted.

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
22	Article 56 (5) "Provisions on transfer of personal data"	Article 184 (2) the PDP Authority Agency may determine a list of countries with higher level of personal data protection than Indonesia. Questions: (1) would this list of countries be made available to public?; (2) would the agency issue this list periodically?
23	Article 57 (5) "Provisions on imposing of administrative sanctions"	• Article 223 (2) stipulates that appeal submission against the administrative penalty sanctioned by the PDP Authority Agency does not lay any ground for the Personal Data Controller to delay the implementation of administrative penalty. This could be problematic if the administrative penalty was in the form of monetary fine, and then the appeal is granted by the PDP Authority Agency. The chance of the money to be returned by the regulator to the Personal Data Controller is almost zero, if not impossible because the money has been deposited as the state's revenue. • Article 225 (1) the amount of administrative fine is up to 2% of the company's annual revenue relevant to the variable of breach(es). For global companies this poses a risk, as it is not clear on whether the revenue in question is limited to the revenues from local market or from the global revenues.
24	Article 61 "Provisions on implementation of the institution's authority"	n/a
25	Article 65	We suggest the clause be reworded to allow for the use of public interest/service as a basis even if there

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
	Public interest or public services cannot be used as a basis for processing where there is a commercial effect or benefit to the data controller .	are incidental commercial benefits (i.e. where the primary purpose is non-commercial).
26	Article 76 (2) This Article sets out the information that a data controller needs to provide, which includes the representative in accordance with regulations and data protection officer contact in accordance with the regulations. It is unclear on who is the representative mentioned in this requirement, especially as there is a separate requirement for the details of the data protection officer.	We seek further clarification on the requirement to name a representative, in addition to naming the data protection officer.
27	Article 82 on verification of accuracy of personal data	While international standards require data controllers to take reasonable steps to ensure that the personal data they process is accurate and kept up-to-date, as well as rectify data on request they do not impose such detailed obligations to verify the accuracy of personal data. The verification obligations will likely place an onerous burden on companies, particularly with regard to data that may be collected for online advertising, or from third-parties. Verification may be warranted in some instances (e.g., to check the age of customers who are purchasing restricted goods), but not all. We

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		recommend amending Art. 82 to reflect the principle of proportionality as is required for such measures.
28	Article 90 (1)	This article seems to require that the controller grant the request for access in all cases, without need for review of the basis and viability of the request. We recommend that the same factors in Article 91 (3) would also apply to requests under article 90, allowing a data controller to reject the request. Alternatively, we seek further clarification if there should be a separate review / appeal process for a data subject's request.
29	Article 99 on notification of deletion/destruction of data	The Draft Implementing Regulation would require data controllers to notify data subjects that their personal data has been deleted or destroyed even if the data has been routinely deleted as part of a retention policy, and not at the active request of the data subject. This would place a significant compliance burden on companies as they need to contact every data subject every single time personal data about them is deleted or purged in accordance with a records retention policy. We recommend that the provisions clarify that such notice is only exercised when the data subject is exercising their rights under Art. 96 and not for routine deletion exercises as may be required under a data retention policy.
30	Articles 115-120 on Lawsuit and Receipt of Compensation	We do not recommend giving personal data subjects the statutory right to demand compensation from personal data controllers or processors for violations of personal data protection regulations. Requiring companies to maintain a process and policy to address compensation requests is administratively burdensome. Rather, such disputes should be adjudicated in court and according to due process

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		and the rule of law. To the extent KOMINFO's aim is to encourage out-of-court settlements for breaches of data protection regulations, this option is generally available to parties even without a statutory right. Even in jurisdictions that provide a private right of action, the international norm for privacy legislation does not give rise to an automatic right of compensation. Further, enforcement of such provisions has been limited to actual losses suffered. For instance, the Court of Justice of the EU decided in May this year that infringements of the GDPR do not automatically give rise to a right of compensation. Instead, the data subject bringing the case must prove that there was harm done to them. This is opposed to Art. 117(a) of the Draft Implementing Regulation which states that personal data subjects do not have to prove any loss suffered. Similarly, the Singapore Court of Appeal found that a mere loss of control of personal data by the data subject did not constitute a "loss or damage" under the SG PDPA, and required a finding of actual loss. We thus recommend that if KOMINFO were to nonetheless include a private right of action, that the data subject must first prove that they have suffered a loss as a result of the PDP violation. While Art. 115 clarifies that a personal data subject's right to sue is based on the fault of the Personal Data Controller, the subsequent provisions refer to the "Personal Data Controller and/or Personal Data Processor" which suggest joint and several liability between these entities. Joint and several liability regimes unfairly prejudice personal data processors that provide adequate protection for personal data and do not process personal data outside or contrary to the instructions of the personal data

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		controllers. We thus recommend that Arts. 117, 118 and 120 are removed.
31	Articles 121 and 122 on Portability and Interoperability of Personal Data	We support the principle of providing a right to data portability and acknowledge the benefits it brings to consumers and businesses. A "one-size-fits-all" approach with respect to data portability cannot efficiently apply to the variety and complexity of services and data sets that exists in the market. Complex data systems are not capable and never will be capable of allowing a "plug and play" type scenario for ingested data. Organizations do not typically process personal data following a particular standard/harmonized format. A broad implementation of the data portability right may stifle competition and innovation and impose unnecessary burdens on organizations. It may require substantive and unrealistic efforts from personal data controllers in order to have the technical systems in place facilitating the data portability right. We recommend that KOMINFO should clearly establish the objectives and aims of such a data portability framework. We also recommend that KOMINFO avoid the introduction of mandatory broad data portability requirements and instead work with the industry to developing voluntary industry best practices, and support and align to regional or international standards and codes of conduct. Data portability frameworks should also be flexible and allow industry to use commercially negotiated terms and conditions offering customers tools and methods to move their data; easy contract termination provisions and pay as you go pricing – which would help addressing any potential "lock-in" concerns. We believe that mandated data portability, when tied to a specific process or standard may threaten innovation and contractual

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		freedom, which in turn may adversely affect market development and harm consumers.
32	Articles 124-126 on notification of failure to protect personal data	We recommend that notifiable data breach notification frameworks be clearly scoped to unauthorized disclosure of, or access to, personal data that may cause material risk of harm, wherein there is material risk of identity theft or economic loss to the data subjects. Incorporating a "materiality" standard is necessary, as it will ensure that notifications, made to the PDPI or data subjects only pertain to breaches that require their greatest attention and expedient mitigation. Without such a threshold, numerous immaterial notices will be issued resulting in "notification fatigue." This would in turn lead to inconvenience for data subjects, increase in administrative costs and burden for the PDPI, and most importantly result in a very real possibility that data subjects and PDPI will fail to take appropriate action in response to notifications that indicate a real risk of harm.
33	Article 127	The article only restates the examples of high risk processing activities for which a PDP impact assessment needs to be conducted (in PDP Law Article 34). We suggest that the regulations provide more specifics of the examples, and align them with generally accepted principles on which activities require an impact assessment (e.g. GDPR).
34	Articles 134-135 on Data Controller's mandatory obligation to audit Data Processor	We recommend the article to recognize the Data Processor's independent auditor attestation to avoid duplicative effort in conducting audit. Data Controller can leverage the independent party's attestation over the Data Processor's control effectiveness in the data privacy and data protection implementation as covered by SOC2 with Privacy Criteria Considerations or ISO27701 on Privacy Information

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		Management System which reflect best practices. This practice is recognized by FSI regulator such as OJK.
35	Articles 156-159 on obligations of the personal data processor	As Art. 155 of the Draft Implementing Regulation correctly points out, personal data processors should only process personal data on orders of the personal data controller. As the personal data controller is the party in the processing who has direct access to and contact with the personal data subject, it is not possible for a personal data processor to ensure accuracy, completeness, or consistency of the data, nor conduct verification as that would entail reaching out to the data subject involved. We thus recommend that Art. 156 is removed. Further, as the personal data processor is only acting on the orders of the personal data controller, keeping a record of processing which was already documented in the agreement creates a duplicative process without affording additional protections for the personal data being processed. We thus recommend that Art. 157 is removed. In addition, personal data processors do not decide what and how personal data is being processed. These are determined by the personal data controller. Also, providers of certain types of services that allow users to process data (e.g. enterprise payroll management solutions, productivity tools, and cloud services) have no visibility over the personal data that their users choose to process. Therefore, it is the personal data controllers – not personal data processors – who are in the position to determine the appropriate level of security to protect the personal data and to maintain confidentiality of the personal data. We thus recommend that Arts 158 and 159 are removed. However, if KOMINFO chooses to retain these Articles, we recommend that provisions be added to

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		clarify that that these Articles apply to personal data processors only to the extent that the specified obligations fall within the personal data controller's instructions to the personal data processor so that it does not conflict with Art 155(1).
36	Articles. 84, 89, 90, 99, 104, 110, 111, 114, 118 on timeframe for data controllers to respond to data subject requests	The international norm for timeframe within which a data controller must respond to data subject requests (e.g. access, correction, deletion) is typically 30 days. This is because businesses require time to receive, assess, and respond to the requests of the data subject. Further, a larger business/data controller may receive numerous queries daily, rendering the 72 hour timeframe for response onerous for compliance
37	Article 166 on appointment of DPO	Data protection laws should avoid imposing requirements that generate unnecessary administrative burdens on organizations, without providing additional protection for the data subject. Art. 166 requires the personal data controller and/or personal data processor to appoint a DPO taking into account the structure, size and organizational needs of the personal data controller and/or personal data processor. Such requirement also increases the cost of operations for organizations and reduces the ease of doing business in Indonesia. We thus recommend that Art. 166 is removed.
38	Articles 183-188 on adequate and binding protection of personal data	We support KOMINFO in ensuring that personal data can be transferred abroad securely and in recognizing that companies are able to ensure that adequate and binding protection of personal data. However, we recommend that KOMINFO recognizes additional ways a company may be bound to protect personal data, such as through internationally recognized standards such as ISO certifications or SOC2 with Privacy Criteria considerations.

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		We recommend expanding the number of legal bases which allow international transfer that is more aligned with international norms and frameworks. Assessment by the DPA should reflect international best practices. We also recommend that any standard contractual clauses that will be determined in a subsequent regulation by the PDPI should align with the equivalent standard contractual clauses under the GDPR. This is important not only to ensure an equivalent standard of privacy protection for personal data transferred overseas, but also to promote harmonized international standards, reduce the compliance burden on global organizations which have already updated their contractual clauses to comply with GDPR requirements, and avoid confusion for organizations and individuals. In addition to ensuring an equivalent standard of data protection for personal data transferred overseas, harmonizing Indonesia's data protection regime with international standards helps boost Indonesia's competitiveness as a business destination. Further, we strongly recommend KOMINFO to carry out thorough and robust consultation with all relevant stakeholders prior to the formulation of the standard contractual clauses. This will ensure that the standard contractual clauses will be technically feasible and cognizant of the interests of all stakeholders.
39	Article 190 on transfer of personal data based on consent of the data subject	We recommend that cross-border data transfer based on explicit consent of the data subject should not be subject to additional conditions. Among other things, these conditions require such transfer to be non-recurring and to involve a limited number of data subjects, and require the data controller to provide a notification to the PDPI and data subject about the transfer. This is not in line with the GDPR

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		or international best practice, where express consent given by a data subject is in itself a sufficient basis for overseas data transfer.
40	Articles 192, 194, 195 on cross-border data transfer obligations on personal data controllers and/or processors	The obligation to record data transfers and ensure that data transferred is sufficient, relevant and limited (Art 192), and to provide a notification with prescribed information about the data transfer to the data subject (Art 195) should be placed solely on personal data controllers that control and determine the purposes and means of processing personal data, including its transfer overseas. We thus recommend that personal data processors be removed from the scope of Arts. 192 and 195. Further, the obligation on personal data controllers and/or personal data processors to carry out a data transfer impact assessment will result in additional administrative burden and operating costs for organizations in practice. It will also be resource-intensive for government authorities to manage and review an enormous number of administrative processes in the form of impact assessments. We thus recommend that Art. 194 is removed. Alternatively, we recommend that any cross-border transfer impact assessment be submitted to the regulator only upon request, as opposed to mandatorily in every case.
	Article 213	The draft lacks clarity on factors that must be taken into account when assessing administrative fines, including the nature and gravity of the infringement, intent, mitigation efforts, responsibility, cooperation, and more. We encourage the government to **determine criteria for violations that are clear, specific, and have proportional weighting for the imposition of administrative sanctions in the relevant**

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		article(s). This is to create legal certainty for Personal Data Controllers and Personal Data Processors without reducing the deterrent effect of administrative sanctions.
41	Article 223	Administrative Appeal Mechanism still lacks clarity on outcomes of objection process and the independence as well as accountability of the decision-making process for appeal • We recommend that the government more **clearly define the various outcomes of the objection process**, such as reduction of fines, repetition of inspections, and revocation of decisions, not currently found in Article 223. • We encourage the government to more **clearly and decisively stipulate the independence and accountability of the objection decision-making process**, among others by adding provisions related to the separation of powers in the objection decision-making process at the DPA.
42	Article 224	During the deliberations of the Personal Data Protection Law, **there was a mutual understanding between the government and parliament that the maximum size of administrative fines refers to two percent of income or revenue *from Indonesia*.** The draft has not reflected this and Article 225 (1) can still be interpreted to mean global revenue. Additional considerations are necessary to ensure that the amount of the fine is as proportional as possible to the violation committed by the Personal Data Controller or Personal Data Processor. • We seek further clarity to define the maximum of two percent of the data

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
		controller's annual income or annual revenue **generated from activities within the jurisdiction of Indonesia.** • We encourage the **inclusion of violations based on negligence and those driven by intentionality.** This distinction can help determine the severity of fines, with intentional violations receiving higher penalties.
43	Articles 200(n), 219(3)(b)-(d) on powers of the PDPI	We are supportive of the set-up of an independent data protection authority. The authority should be empowered to receive complaints and carry out investigations. We recommend that rule-making powers of the government and the authority be scoped reasonably, clearly, and consistent with enabling rule and regulation making. Over-broad discretionary powers should be avoided, such as the right to carry out inspections and searches to electronic systems, facilities, rooms, and/or places used by the personal data controller and/or personal data processor, including obtaining access to data, as it creates uncertainty in implementation and increases the cost of compliance. We strongly support the inclusion of clear due-process mechanisms, including an explicit provision for the relevant authority to carry out thorough and robust consultation with all relevant stakeholders, prior to the formulation of any rules. This will ensure that the emergent rules will be technically feasible, cognizant of the interests of all stakeholders, including data subjects and consistent with the government's digital economy objectives, and the aims of protecting data. We thus recommend that Arts. 200(n) and 219(3)(b)-(d) are removed.
44	Chapter XX	We recommend that the form of the agreement between the data controller and data processor

SNo.	Articles in PDP Law and key issues	Detailed Comments and Recommendations
	Under Article 137 (2) of the Draft PDP Regulation, the agreement between data controller and data processor must use Indonesian language. It is unclear on how this will be applied considering that under the current practice, any agreement entered between foreign party and an Indonesian party can still be presented in bilingual form (i.e., Indonesian and foreign language) where the parties can also agree that the governing language is the foreign language. As such, further clarification may be needed from the authority on this point.	follow the general principles of contract law in Indonesia which allows for bilingual agreements.