September 14, 2023

BSA COMMENTS ON DRAFT IMPLEMENTING REGULATION OF LAW NUMBER 27 OF 2022 REGARDING PERSONAL DATA PROTECTION

Introduction

On behalf of BSA | The Software Alliance (**BSA**),[1] we thank you for soliciting feedback from the private sector on the Draft Implementing Regulation of Law Number 27 of 2022 Regarding Personal Data Protection (**Draft PDP Regulation**). We welcome the opportunity to submit comments to the Ministry of Communication and Informatics (**KOMINFO**). In past years, BSA has provided comments in joint submissions: on the Draft Personal Data Protection Bill in 2019,[2] and the Draft Amendment of Government Regulation 82/2012 on Electronic Systems and Transaction Operations in 2018.[3] Most recently in March 2023, we met with officials from KOMINFO on the sidelines of the Initiative Indonesia Financial Services and Information Technology Mission.

BSA is the leading advocate for the global software industry. Our members are enterprise software companies that create business-to-business technologies that help other businesses innovate and grow. For example, BSA members provide tools including cloud storage and data processing services, customer relationship management software, human resource management programs, identity management services, and collaboration software. BSA offers our extensive global experience in technology policy to serve as a resource and we hope that our comments in this submission will be helpful to KOMINFO.

Allow sufficient time for engagement with private sector

BSA reiterates our appreciation to KOMINFO for conducting the public consultation. We respectfully suggest enhancing the engagement process by extending the timeframe for public input. In comparison to other jurisdictions in the region — which typically provide timeframes of at least one to two months for considerably shorter draft documents — allowing a longer timeframe for the review of the extensive Draft PDP Regulation would facilitate a more detailed examination. Establishing longer consultation periods would also enable industry stakeholders to provide detailed feedback on specific recommendations, leading to a comprehensive engagement that may better assist KOMINFO as it revises the regulations to achieve the regulatory goals. Moreover, clearly communicating the timelines and milestones for the public consultation process would assist stakeholders in understanding when

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Palo Alto Networks, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] See https://www.bsa.org/policy-filings/indonesia-usabc-bsa-comments-on-draft-indonesia-personal-data-protection-bill

[3] See https://www.bsa.org/policy-filings/indonesia-bsa-joint-submission-on-gr82-amendment-matrix

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

the PDP Regulation will be published and the expected timeframe for subsequent implementation. Such clarity would contribute to an efficient and transparent regulatory process in which stakeholders can provide more meaningful feedback to KOMINFO.

BSA appreciates the opportunity to provide our initial comments on the Draft PDP Regulation. However, due to the limited time available, our comments are focused on the most pressing concerns. With a more thorough review of the Draft PDP Regulation, additional concerns are likely to surface. Therefore, we kindly request the opportunity to engage in further discussions and provide more comprehensive comments beyond the September 14, 2023 deadline. Extended dialogue would enable us to contribute more fully to the development of the Draft PDP Regulation.

Duplication between the PDP Law and the Draft PDP Regulations

The efficiency and clarity of the Draft PDP Regulations could be enhanced by, where possible, minimizing duplication between the Law Number 27 of 2022 Regarding Personal Data Protection (**PDP Law**) and the Draft PDP Regulations. Several provisions of the Draft PDP Regulations repeat, in either similar or slightly different terms, provisions of the PDP Law. Following is a non-exhaustive list of these repetitions:

- Article 1 of the Draft PDP Regulation and PDP Law both contain definitions; where these definitions are identical, they should be removed from the Regulations. Where they may be divergent, parties may become confused about which definition applies;
- Article 2 of the Draft PDP Regulation and PDP Law both set out the application and scope of the respective document;
- Article 5 of the Draft PDP Regulation effectively expands the definition of Personal Data;
- Article 6 of the Draft PDP Regulation and Article 4 of the PDP Law both set out the distinction between “specific” and “general” Personal Data; and
- Article 9 of the Draft PDP Regulation and Article 16 of the Law both set out the definition of “Processing”.

BSA would very much welcome the opportunity to meet KOMINFO to discuss these, and other, duplications and how the structure of the Draft PDP Regulations could be optimized to promote clarity and certainty for stakeholders.

Extraterritoriality

Article 2(1)(b) of the Draft PDP Regulation states that it regulates “Any Person, Public Agency and International Organization that perform Personal Data Processing outside of the jurisdiction of the Republic of Indonesia, which has legal consequences in the jurisdiction of the Republic of Indonesia; and/or to the Indonesian citizen Personal Data Subject outside the jurisdiction of the Republic of Indonesia.” Article 2(1)(b) does not define what could constitute “legal effects or consequences” in the context of applicability within the jurisdiction of Indonesia and Indonesian citizens outside Indonesia. BSA recommends streamlining the extraterritorial application envisaged under the PDP Law, specifically to include within the Draft PDP Regulation a definition of “legal effects or consequences” that is restricted to the provision of goods and services by any person outside of Indonesia, with the intent of targeting individuals within Indonesia or similarly targeting Indonesians based abroad.

Roles and responsibilities of Data Controllers and Data Processors

BSA appreciates the introduction of the concept of Personal Data Controller and Personal Data Processor within the Personal Data Protection Law and the Draft PDP Regulation, which is aligned with many privacy regulations around the world. We recommend further refinement of the roles and responsibilities assigned to Personal Data Controllers and Personal Data Processors, including:

- Article 20 recognizes that Personal Data Controllers may designate Personal Data Processors. Under Article 20(2), Personal Data Processors are required to process data "based on the Personal Data Controller's instruction.". However, Article 213 appears to contemplate imposition of administrative sanctions on Personal Data Processors in addition to Personal Data Controllers. Given that Personal Data Processors are required to process data according to the controller's instructions, and controllers are required to determine the purposes and controls of processing, BSA recommends amending the Draft PDP Regulations so that Personal Data Processors are not subject to sanctions when they are acting based on the Personal Data Controller's instruction.

- Article 156(1)-(2) stipulates that the Personal Data Processor must ensure the accuracy of Personal Data, including conducting verification of the data. However, Personal Data Processors typically do not have a direct relationship with Personal Data Subjects and often do not have access to the data they maintain on behalf of a Personal Data Controller, making it challenging for them to directly ensure the accuracy of personal data. In some cases, Personal Data Processors may even be contractually prohibited from looking into or accessing the data they process on behalf of a Personal Data Controller, and therefore, would not be able to ensure the accuracy of such personal data. We recommend deleting this provision.

- Articles 192 and 194 require both the Personal Data Controller and Personal Data Processor to record and map the transfer of personal data outside of Indonesia, essentially conducting a data transfer impact assessment. We suggest revising these provisions to only require one entity to conduct any such assessment, to avoid repetition when a Personal Data Processor acts on the instructions of a Personal Data Controller. In that scenario, it is sufficient for the Personal Data Controller to carry out the data transfer impact assessment.

- Article 195 requires the Personal Data Controller and/or the Personal Data Processor to provide information to the Personal Data Subject prior to the transfer of personal data. Again, we recommend amending the Draft PDP Regulation such that the Personal Data Controller is responsible for doing so because the Personal Data Controller is generally the entity who has a direct relationship with the Personal Data Subject.

In summary, BSA recommends that Articles 156(1)-(2), 192, 194 and 195 require only the Personal Data Controller to be responsible for the obligations within as the Personal Data Controller is the appropriate party to take on those obligations. For more insights on how the roles and responsibilities of data controllers and data processors should be distinguished, please refer to BSA's paper titled "The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation." [4]

[4] See https://www.bsa.org/policy-filings/the-global-standard-distinguishing-between-controllers-and-processors-in-privacy-legislation

Consent and additional bases for processing

The PDP Law creates six legal bases for companies to process personal data. We recommend three changes to the Draft PDP Regulation's treatment of these bases for processing.

First, Article 14(d) requires that the Personal Data Controller must limit disclosure of personal data to a purpose that has been approved by the Personal Data Subject. This requirement could disrupt processing that is conducted under other legal bases, including the fulfillment of agreement obligations with the Personal Data Subject, the fulfillment of legal obligations of the Personal Data Controller, among others, as set out in Article 20 of the PDP Law. BSA suggests amending Article 14(d) so that the Personal Data Subject must approve disclosures of personal data only where data subject consent is the legal basis for processing.

Second, Article 54(5) states that a contractual agreement cannot be deemed to replace the position of consent as a legal basis for processing, and Article 54(6) states that a Personal Data Controller remains obliged to use consent as a legal basis for processing to carry out the processing activity that needs consent. Article 55(1) of the Draft PDP Regulation sets out additional obligations when companies rely on agreements, i.e., the fulfilment of contractual obligations, as the basis for processing personal data under the PDP Law. Under the Draft PDP Regulation, even though companies rely on an agreement, it nevertheless includes the need to obtain explicit and lawful consent from the Personal Data Subject. All three Articles contradict the position the PDP Law which recognizes contractual necessity as an independent bases for processing personal data. This creates confusion and ambiguity for businesses and consumers alike.

BSA suggests revising these provisions to avoid requiring companies to additionally obtain consent to process data when they are already processing that data on the basis of another ground for processing recognized in Article 20 of the PDP Law. As written, the Draft PDP Regulation is overly reliant on consent, and will result in individual data subjects receiving a variety of consent requests even when companies are processing their data pursuant to a separate existing agreement. This result is contrary to the PDP Law, which recognizes consent and contractual necessity as independent bases for processing personal data. Therefore, we recommend deleting Articles 54(5)-(6) and 55(1)(a).

Third, Article 71 requires Personal Data Controllers to document and submit the results of the legitimate interest analysis and assessment to the Personal Data Subject. This requirement goes beyond other global data protection laws, which require companies to conduct an analysis of applying the legitimate interest basis for processing — but do not require that analysis be given to an individual Personal Data Subject. Submitting the analysis to the Personal Data Subject can create new privacy or security risks, such as when companies rely on legitimate interests to process data for purposes like fraud detection or cybersecurity, where proactive disclosure around these types of processes could ultimately undermine their effectiveness. BSA therefore recommends deleting Article 71.

Failure of Personal Data Protection

Articles 124 to 126 of the Draft PDP Regulation set out the requirements of the Personal Data Controller to notify stakeholders of failure of Personal Data Protection. The Draft PDP Regulation does not include a definition of a "failure of Personal Data Protection." For clarity, BSA recommends including a definition that is similar to how data breaches are defined in other jurisdictions. For example, the European General Data Protection Regulation (**GDPR**) defines a "personal data breach" as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, while the Singapore Personal Data Protection Act (**PDPA**) defines a "data breach" in relation to personal data as the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

Under Article 124, Data Controllers would be required to report breaches to both the PDP Institution and to individual Personal Data Subjects within three days — even when those breaches have not created significant risks of harm, thus adding unnecessarily complexity to the process. As such, we offer the following for consideration.

Notification of Failure of Personal Data Protection to the PDP Institution

The Draft PDP Regulation requires that personal data breaches are reported to the PDP Institution, and this includes personal data breaches of low risk to Personal Data Subjects. This may result in notification fatigue to both the PDP Institution and to data controllers, which erodes the effectiveness of the notification requirement. BSA recommends that the threshold for notification to the PDP Institution be the unauthorized acquisition of unencrypted or unredacted personal data that creates a material risk of harm to Personal Data Subjects so that the PDP Institution and data controllers can appropriately focus their efforts on such breaches.

Notification of Failure of Personal Data Protection to the Personal Data Subject

Notifying Personal Data Subject about every data breach, regardless of its significance, is counterproductive. Such a practice could lead to unnecessary alarm in cases of inconsequential data breaches, or notification fatigue among Personal Data Subjects where they fail to take necessary steps to safeguard their own personal data even in serious cases. Therefore, BSA recommends a more selective notification requirement, where notifications are required only when there is a significant negative impact on the Personal Data Subject.

Timeline for Notification to PDP Institution and Personal Data Subjects

While we support prompt notification of breaches that create significant risks of material harm to individuals, we strongly suggest revisiting the requirement for a strict 3 x 24-hour timeline for notification. Complying with such a stringent timeline could divert valuable resources towards reporting and communication efforts instead of focusing on rectifying the data breach. Therefore, we propose a more flexible timeframe that allows data controllers the autonomy to effectively manage both the breach and the notification process. Specifically, we recommend that the 3 x 24 hour timeline to notify the Personal Data Subject and PDP institution be amended to notification made "without undue delay."

Cross-Border Data Transfers

The Draft PDP Regulation also implements the PDP Law's restrictions on cross-border data transfers. We recommend three revisions to this aspect of the regulations:

- First, Article 185(2) of the Draft PDP Regulation specifies mechanisms for the cross-border transfer of personal data for ensuring "Adequate and binding Personal Data Protection." BSA proposes including certifications as valid mechanisms to create more flexibility in supporting cross-border data transfers. Internationally recognized certifications such as the ISO 27701, the Global and APEC Cross Border Privacy Rules (**CBPR**) and other such certifications should be recognized to allow the transfer of personal data outside Indonesia. These certifications have proved beneficial for companies that operate across national boundaries in demonstrating their compliance with globally interoperable and trustworthy data privacy standards.

- Second, Article 187 allows the PDP Institution to determine standard contractual clauses. BSA recommends that the PDP Institution consider recognizing other widely accepted standard contractual clauses, such as the EU Standard Contractual Clauses (**SCC**) and ASEAN Model Contractual Clauses (**MCC**). Approving the use of standard contractual clauses recognized in other jurisdictions would allow Personal Data Controllers to serve customers in Indonesia using existing contracts that create strong data protection obligations and are aligned with established international practices. BSA further recommends that the PDP Institution carry out a public consultation to gather industry comments prior to releasing approved standard contractual clauses.

- Finally, Article 188(3) requires a Personal Data Controller to obtain approval from the PDP Institution before transferring personal data when using binding corporate rules (**BCRs**) as a cross-border data transfer mechanism. We recommend the PDP Institution recognize that BCRs that have already received approval from other data protection authorities may be

considered acceptable data transfer mechanisms under the PDP Law without the need for separate approval from Indonesian authorities.

Enabling data controllers to use different mechanisms to transfer personal data across international borders affords businesses the flexibility to determine the mechanisms that will be most optimal and relevant for them. In summary, BSA recommends recognizing more mechanisms for cross-border personal data transfers, including certifications, standard contractual clauses from other regions, and BCRs approved in other jurisdictions.

Responding to Data Subject Requests

Articles 84, 89, 90 and 99 require Personal Data Controllers to respond to Personal Data Subject requests in relation to correcting, granting access to, providing a copy of, and deleting personal data within a period of no later than 3 x 24 hours. This is an insufficient timeframe for Personal Data Controllers to adequately respond to Personal Data Subject requests, which can vary significantly in volume and scope. BSA recommends that the timeframe in which Personal Data Controllers are required to comply with Personal Data Subject requests should be revised to be in line with practices in other jurisdictions. For example, the GDPR requires the data controller to respond to consumer rights requests without undue delay and within one month of the request, with an option to extend the time limit by two further months, and the option for the data controller to charge a reasonable fee or refuse to grant the request in some cases.[5] The Singapore PDPA requires an organisation to respond to Personal Data Subject requests as soon as reasonably possible, within 30 days.[6] BSA recommends requiring Personal Data Controllers to respond to Personal Data Subject requests without undue delay and within 30 days, with an option to extend the time limit by two further months by informing the Personal Data Subject, and to refuse to grant the request in cases where the request is unfounded or excessive.

Compensation mechanism

The provisions under Articles 117-120 require Personal Data Controllers to set up and implement compensation mechanism, policy, and processes whereby Personal Data Subjects can claim and receive relevant compensation amounts directly from a Personal Data Controller, upon submitting evidence of nominal or non-material losses for any personal data protection failures. This provision risks opening a spate of unfounded submissions, which would add unnecessary burden and costs to Personal Data Controllers. Further, Article 117(a) states that the Personal Data Subject must submit evidence of a violation of the processing of Personal Data which has an impact on the Personal Data Subject, without having the prove the losses suffered by the Personal Data Subject. BSA recommends that any claim for compensation should be based on the directions of, or be directed to, the relevant data protection authority, i.e., the PDP Institution. Without appropriate guidance and relevant precedents, such provision may result in considerable legal uncertainty. We further recommend including a requirement for the Personal Data Subject to prove the violation caused actual harm. Finally, BSA recommends deleting "without having to prove the losses suffered by the Personal Data Subject" within Article 117(a).

[5] See Article 12 of the EU GDPR at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

[6] See Section 21(1) of the Singapore PDPA at https://sso.agc.gov.sg/Act/PDPA2012, and Personal Data Protection Regulations 2021, Part 2 at https://sso.agc.gov.sg/SL/PDPA2012-S63-2021.

Conclusion

In the context of the Digital Economy Framework Agreement (**DEFA**) initiated by ASEAN, it is imperative for Indonesia to prioritize the alignment of its regulatory framework with regional objectives. To promote seamless cooperation and foster growth in the digital economy, we recommend that Indonesia carefully assess the Draft PDP Regulation accordingly.

BSA appreciates the opportunity to provide our comments and recommendations on the Draft PDP Regulation. We hope that our comments will assist in the development of clear and rigorous regulations for personal data protection in Indonesia. We look forward to continuing our engagement with KOMINFO and relevant agencies on personal data protection and privacy policies and request that KOMINFO consider further detailed submissions past the stipulated deadline of September 14, 2023. We urge KOMINFO to continue engaging with the private sector on how to further improve the Draft PDP Regulation. **We would like to take this opportunity to offer a meeting at your convenience to discuss the Draft PDP Regulations further**. Please do not hesitate to contact the undersigned at waisanw@bsa.org to continue the discussion.

Yours faithfully,

Wong Wai San

Wong Wai San

Senior Manager, Policy – APAC