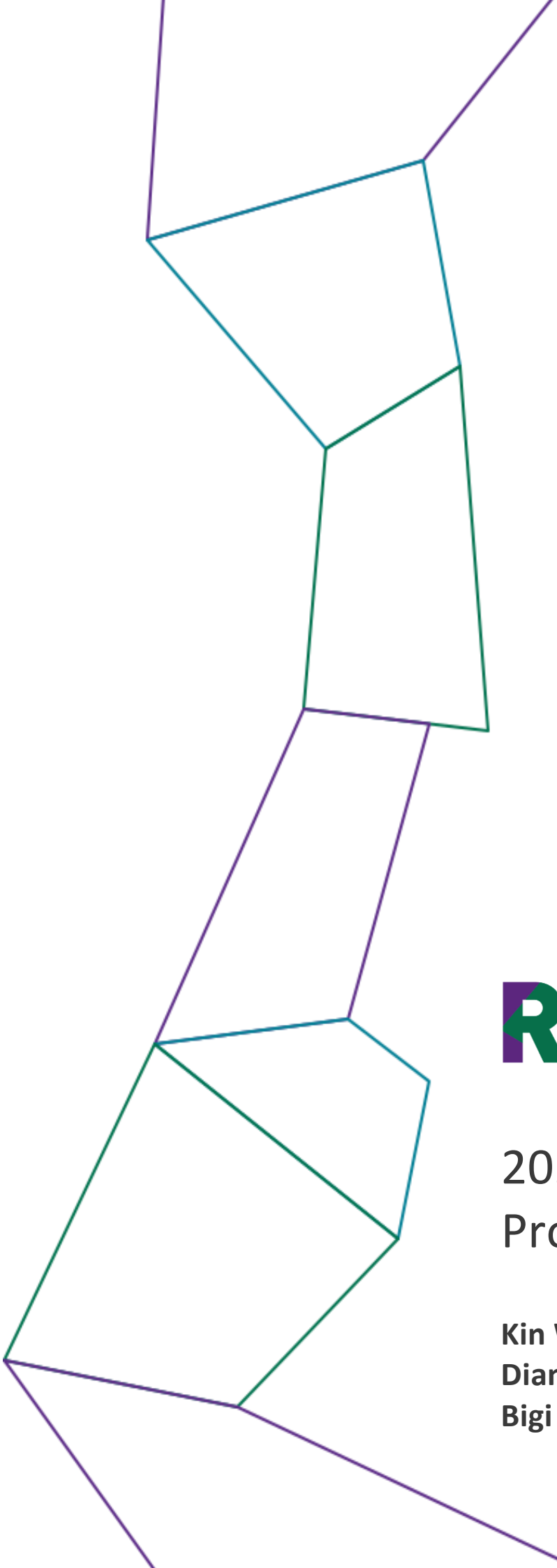

ROUSE

2022 Indonesian Data Protection Law

Kin Wah Chow
Dian Esterina Tambunan
Bigi Ramadha Putra

2022 INDONESIAN DATA PROTECTION LAW OVERVIEW

The Indonesian government, on 17 October 2022, passed Law No. 27 of 2022 concerning Personal Data Protection Law (the "**PDPA**"). This article seeks to give an overview of the 2022 Indonesian Personal Data Protection Act (PDPA).

The following topics will be discussed:

a) Principles for data processing
b) Legal basis for data processing
c) Obtaining consent from data subject
d) Accuracy and updating personal data
e) Data breach
f) Data processor
g) Transfer of data outside Indonesia
h) Data Protection Impact Assessment
i) Data protection officer
j) Sanction for beaches
k) Grace period for implementation

The Indonesian law is touted to be modeled on the EU GDPR, however there are differences and legal advice should be sought when adapting privacy policy for Indonesian residents.

Principles of data processing

Similar to the GDPR, Article 16 Paragraph (2) of the PDPA provides for the following principles of data protection:

- Lawfulness principle
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- integrity and confidentiality

Legal basis for data processing

Article 20 Paragraph (2) PDPA which mirrors Article 6 of the General Data Protection Regulation (GDPR) sets out potential legal bases for data processing, namely: consent; contract; legal obligation; vital interests; public task; or legitimate interests.

Consent

The key principle is that data can only be processed according to the purpose(s) for which data subjects have consented to. Articles 22 – 24 PDPA address the requirement for obtaining consent.

The provision requiring consent from data subject appears similar to those under GDPR to some extent.

However, the PDPA does not clarify whether click wrap method of recording consent will be recognized. This can be a concern because Indonesian judges still take a traditional view of valid agreement as a document containing the terms of agreement with wet ink signature on the document. Of late, regulations have been passed to allow for electronic signatures where the users have enrolled with local certifying authority to certify such signatures. The regulations also recognize uncertified signatures (Article 60, Government Regulation No. 71 of 2019 on Administration of Electronic Systems and Transactions). As it stands now, the legal framework recognizes certified electronic signature and uncertified electronic signature (coming to mind would be DocuSign). However, there is still uncertainty in the legality of signifying assent to terms and conditions using click wrap method.

The current regime does not clearly support click wrap consent where there will be no record of signature signifying agreement or acceptance to be bound by certain terms and conditions. Data controllers should seek professional advice on how best to capture the data subjects' consent to the privacy policy. Web based businesses with Indonesian users may wish to seek legal advice on how best to address this issue.

Disclosure in consent

The disclosure necessary for obtaining consent is set out in Article 21 of PDPA - key information includes:

- The purpose of Personal Data processing
- The retention period of documents containing Personal Data
- The details regarding the Information collected
- The period of Personal Data processing
- The rights of the Personal Data Subject

The data subject needs to be notified of any change in the above.

Accuracy and updating

Under one of the principles discussed above, data controllers are obliged to process data "in an accurate, complete, not misleading, up-to-date and accountable manner". Article 29 of PDPA obliges the data controller to conduct verification of data

Data controllers are required to update and correct errors in personal data within 72 hours after receiving the request for such updates/corrections - Article 30 of PDPA.

In this regard, note that the Data Controller must provide access to data subjects within 72 hours upon request from data subjects – Article 32 PDPA.

Data breach

Data subjects are to be notified within 72 hours of any data breach - Article 46 of PDPA Law

Data processor

Although the PDPA acknowledges the role of data processors, data controllers still have the duty to supervise data processors (Article 37 of PDPA). Responsibility to prevent unauthorized access still remains the responsibility of the data controller (Article 39 of PDPA), and this appears to be the case even if a data processor has been appointed.

Transfer of data outside Indonesia

Transfer of data out of Indonesia is permitted if:

a) The destination country has in place data protection Law that is on par or impose "higher" than Indonesia's data protection law; or
b) Data controller ensures that "there is adequate and binding personal data protection"; or
c) Obtain consent of data subject.
d) Presumably means that the data controller needs to at least have in place adequate assurance from the overseas entity that is receiving the data. This should be looked at on a case-by-case basis.

Data Protection Impact Assessment

Data Protection Impact Assessment is required under Article 34 of PDPA when there is "potential of high risk" in the processing of personal data. Although this requirement seems to be inspired by GDPR requirement, it seems to have gone broader in coverage - impact assessment is considered as of “high risk potential” under Article 34(2) when “processing personal data on large scale" or when the processing involves "matching or combining groups of data".

These descriptions without further qualifications seem potentially broader in scope – broader than the scope contemplated by the EU GDPR. It is however clear that processing of certain sensitive data (referred to as Specific Data) will require impact assessment.

Such data includes health data; biometric data; genetic data; criminal record; children’s data and personal financial data. Of practical interest will be “children’s data” which suggest personal data collected from minors. This might be particularly relevant to gaming related websites.

Article 34(3) provides for further implementing regulations which hopefully would clarify when such data impact assessment is required.

Data protection officer

Data controllers are required to appoint a data protection officer – Article 53 of PDPA. At this point, there is no registration requirement of the data officer. However, the relevant provision provides for further implementing regulations to be passed with respect to appointment of data protection officer.

Sanctions

The PDPA creates the following offences that are punishable by fine and/or imprisonment:

- unlawfully obtains or collects Personal Data that do not belong to them with the intention to benefit themselves or other persons (Article 67(1) of PDPA)
- intentionally and unlawfully discloses Personal Data that does not belong to them (Article 67(2) of PDPA)
- who intentionally and unlawfully uses Personal Data that does not belong to them (Article 67(3) of PDPA)
- intentionally create false Personal Data or falsify Personal Data with the intention to benefit themselves or other persons (Article 68 of PDPA)

Management and/or beneficial owners could also be liable under these provisions (Article 70 Paragraph (1) of PDPA).

The specter of criminal sanction underscores the need to have in place the framework of proving that consent for collection of data has been secured – see discussion above regarding click wrap and consent.

The aggrieved party may seek compensation from the defaulting data controller – Article 12 of PDPA.

The court may also impose sanctions such as payment of compensation, suspension of business, confiscation of profits, partial or complete shutdown /cessation of business, dissolution of the company (Article 70 Paragraph (4)). In the case of fine, the amount can be up to two (2) percent of the company turnover (Article 57 Paragraph (3) of PDPA).

The sanction of imprisonment is one significant area where the Indonesian PDPA departs from EU's GDPR which provides for administrative fine, correction order and compensation but not imprisonment.

Grace period

Data controllers have two years from the passing of the law (17 October 2022) to comply with the provision of the PDPA.

What businesses should do

Businesses should immediately review their respective privacy policy to ensure that the privacy policy does not conflict with the PDPA.