SQUIRE PATTON BOGGS

Data Protection in Indonesia

Indonesia's Ministry of Communication and Informatics is in the process of enacting a more specific data protection law that may lead to a paradigm shift in data privacy in Indonesia.

The current legal framework that protects personal data in Indonesia uses a broad-brush approach without going into specific guidelines.

On December 1, 2016, the Ministry of Communication and Informatics issued a regulation specifically aimed at protection of personal data contained in an electronic system, yet to be made into law by the Parliament (Regulation 20 of 2016, referred to as "Draft Law").

Notable Provisions in the Draft Law

Differentiating Between General Personal Data and Specific Personal Data

Specific personal data is data that requires special protection, either directed by other laws and/or regulations or relating to specific personal information. Examples of this type of data include religion, health, physical and mental condition, biometrics, genetics, sex life, political views, criminal records, child data and personal financial information. General personal data is all data that is not "specific personal data", but that can be obtained from the public domain or has been disclosed under an identity document. Examples of this type of data include name, email address, photo, identity card number and date of birth.

Differentiating Between Personal Data Controller and Personal Data Processor

Personal data controllers are the parties that obtain data from the personal data owner and, therefore, must obtain consent from the same; personal data processors are those that process the personal data on behalf of a personal data controller. Personal data controllers are obligated to ensure that the scope of consent allows the personal data processors to process the said data. Processing of data includes acquiring and collecting, processing and analysing, storing and displaying, fixing and renewing, announcing and delivering, distributing and disclosing, and deleting and/or destroying.

Consent Requirement and Use of Personal Data

Under the Draft Law, use of **any** personal data, general or specific, requires written and informed consent, except if the use is for the data owner's data security protection, for medical purposes, for law enforcement purposes and as required under laws and regulations.

As for personal data in general, consent is not required if the use of personal data is mandated by law, required to perform a contract or an agreement, and/or required to protect the personal data owner from any threat to their life or their physical or economic wellbeing.

Data Transfer

Consent from the personal data owner is essential before any transfer can be done within Indonesia. In case of cross-border transfers, the receiving country must also have some personal data protection laws and there must be a contract with the offshore third party.

Notification on Breach of Personal Data

Personal data owners must be informed if their personal data has been disclosed inadvertently within 14 days after the data breach is known. The notice must contain the disclosed data, circumstances of disclosure and actions taken to mitigate such disclosure.

Requirements to Delete or Destroy Personal Data

Data must be deleted or destroyed, depending on its nature, under certain circumstances. This includes situations where the data no longer possesses usage value, expires or becomes irrelevant, or the owner of such data withdraws consent to continued use of such data.

Strengthening Privacy Protection

The new law includes provisions regulating processing devices, visual data processors and closed-circuit television. Operators of these devices must provide information if there is such a device installed in an area for purposes other than a criminal investigation. Additionally, personal data owners can, at any time, make a written request to the personal data controller to stop using their personal data for direct marketing activities.

Commission

The Draft Law introduces a regulatory body, i.e. a commission, to ensure that its provisions are complied with. The commission will primarily be responsible for monitoring compliance, facilitating dispute resolution and giving recommendations on personal data protection breaches and claims.

Impact on Employee Data Privacy

Under the Draft Law, three aspects of employee data management are addressed: retention, offshore transfer of employee data and transfer of employee data to a third party.

- Personal data stored in electronic systems must be stored for at least five years, unless otherwise regulated. After the five year period has elapsed, the personal data may be erased, unless the data is still being utilised according to the initial purpose of its collection.
- Upon termination of employment, relevant employee data should be retained for at least two years after employment termination, in line with the limitation period for employment claims.
- Any offshore or third-party transfer of employee data must be stipulated by the employer in the regulations of the company and consented to by the employee.

Contacts

Biswajit Chatterjee
Partner
T +65 6922 8664
E biswajit.chatterjee@squirepb.com

Kaustubh George
Senior Associate
T +65 6922 8658
E kaustubh.george@squirepb.com

Anandee Banerji
Associate
T +65 6922 8677
E anandee.banerji@squirepb.com

Nabil Shadab
Associate
T +65 6922 8668
E nabil.shadab@squirepb.com