Global Data and Cyber Handbook - Indonesia

Regulators, Enforcement Priorities and Penalties

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: 13 January 2025*

The general regulator for data privacy is the Ministry of Communications and Digital (MOCD). Additionally, sectoral authorities, such as Bank Indonesia and the Financial Services Authority (*Otoritas Jasa Keuangan* - OJK) in the financial sector, regulate specific provisions and requirements applicable only within their respective sectors.

For non-personal data, the relevant authority will depend on the nature of the data. For example, if the data is financial-related, the regulators in the financial sector will oversee such data.

For cybersecurity, the National Cyber and Code Agency (*Badan Siber dan Sandi Negara* - BSSN) is the regulator, along with the MOCD.

Under the PDP Law, the President needs to establish the data protection authority to supervise data privacy issues in Indonesia.

According to the PDP Law, the data protection authority will have the following duties and responsibilities:

Formulate and determine the policy and strategy for personal data protection, as well as guidelines for data subjects, data controllers and processors

Supervise the implementation of personal data protection

Issue administrative sanctions against any violations

Facilitate out-of-court dispute settlements

# How active is each of the regulator(s)?

*Last review date: 13 January 2025*

Moderately active

# What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: 13 January 2025*

The MOCD may carry out random investigations to ensure compliance with the requirements for processing (e.g., collection, transfers or disclosures) of personal data, if triggered by individual complaints. To date, there have been no reports of penalties imposed for data breaches under the PDP Law, as the formula for determining penalties has yet to be established). Additionally, no public statements regarding data incidents have been required since the enactment of the PDP Law.

However, the MOCD has urged all relevant parties to focus on complying with the PDP Law now that the transitional period has ended. Key areas of focus include the legal basis for using personal data, data incident requirements, recording of data processing activities, the role of data protection officers, and the requirements for transfers of personal data.

# What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: 13 January 2025*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

☒  Rare

In current practice, investigations and enforcement are carried out in the event of data breach.

Class actions/group actions under data or cyber regulation are:

☒  Rare

# What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: 13 January 2025*

There are:

☒  administrative remedies / civil penalties applied by regulators and law enforcement

Under the PDP Law, administrative sanctions can be in the form of warning letters, suspension of data processing activities, deletion of personal data, and/or administrative fines. The maximum administrative fine is 2% of the annual revenue against the violation variable (not yet clear on the calculation and the variable).

☒  criminal penalties from regulators and law enforcement

Under the PDP Law, criminal sanctions can be in the form of imprisonment (four to six years) and/or monetary penalty (IDR 4-6 billion, or approximately USD 285,000- USD 430,000). In addition, if the crime is done by a corporation or an entity:

The criminal sanction can be imposed on the management, controller, instructor or beneficiary owner of the entity and/or the entity itself.

The criminal sanction that can be imposed on an entity itself is the monetary penalty.

The monetary penalty that is imposed on an entity is ten times the maximum amount that should have been imposed.

Additional sanctions can be imposed in the form of seizure of revenue and/or assets that are obtained or as a result of the crime, suspension of business activities, permanent ban of business activities, closure of business activities, fulfillment of breach obligations, compensation payment, revocation of licenses, and/or liquidation of the company.

# If data subjects have private remedies, what form can these remedies take?

*Last review date: 13 January 2025*

Not applicable as there is no specific provision on private remedies under the PDP Law.

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.