



Constitutional Court Ruling Means More Firms Must Appoint a Data Protection Officer

Issue 18, September 2025

A recent Constitutional Court ruling has lowered the threshold for when companies must appoint a Data Protection Officer (“**DPO**”) under Indonesia’s Personal Data Protection Law.

The DPO plays a central role in ensuring compliance with personal data protection (“**PDP**”). Article 54 of Law No. 27 of 2022 on Personal Data Protection (“**PDP Law**”) formally introduced the DPO role and outlines its responsibilities:

- (a) inform and **advise** personal data controllers and processors on compliance with the PDP Law;
- (b) **supervise** and **ensure** that controllers and processors comply with the PDP Law;
- (c) provide **advice** and **assess** the impact of PDP, and **monitor** the performance of controllers and processors; and
- (d) **coordinate** and **act as a liaison** on PDP issues.

Recognizing the importance of the DPO’s role, Article 53 (1) PDP Law sets out three specific scenarios where controllers or processors must appoint a DPO:

“Personal data controllers and personal data processors must appoint officials or officers to carry out the personal data protection function in the event that:

- (a) the processing of personal data is for the purposes of public services;*
- (b) the core activities of the personal data controller have a nature, scope, and/or purposes that require regular and systematic monitoring of personal data on a large scale; and*
- (c) the core activities of the personal data controller consist of large-scale processing of personal data that is specific and/or personal data related to criminal acts.*

A small but significant detail of Article 53 (1) is that the scenarios are connected by the word “and”, which in strict legal terms makes the list cumulative. This means all three of the conditions must be met to trigger the legal obligation to appoint a DPO.

Recently however, the Indonesian Constitutional Court (“**MK**”) issued Decision No. 151/PUU-XXII/2024 (“**Decision 151**”), which alters the reading of Article 53 (1) of the PDP Law. The key aspects and background of Decision 151 are outlined below.

A. Background of the Case

Eric Cihanes, a recent law graduate, and Garin Arian Reswara, a law student, (collectively, the “**Petitioners**”) brought a lawsuit before the MK, requesting that Article 53 (1) of the PDP Law be deemed conditionally unconstitutional unless the word “and” is interpreted as “and/or”. Their argument is based on Article 28G (1) of the Indonesian Constitution, which states that: “*Every person has the right to the protection of self ...*”. Citing this provision, the Petitioners argued that personal data protection is an integral part of the constitutional right to privacy, as previously recognized by the MK in Decision No. 5/PUU-VIII/2010.

Building on this, the Petitioners contended that the cumulative formulation of Article 53 (1) unduly narrows the obligation to appoint a DPO. If a data controller or processor meets only one or two of the listed criteria, they would not be required to appoint a DPO. The Petitioners also highlighted that each scenarios in Article 53 (1) qualify as high-risk data processing activities under Article 34 (2) of the PDP Law. They concluded that appointing a DPO in such cases is a form of “heightened supervision” intended to mitigate the risk of PDP violations in high-risk data processing activities.

Concluding their argument, the Petitioners claimed their constitutional rights were violated because the cumulative formulation of Article 53 (1) does not provide an adequate standard of PDP for high-risk data processing, with the use of “and” limiting the scope of protection.

B. MK's Findings in Decision 151

After reviewing the Petitioner’s case, the MK issued Decision 151, which includes the following noteworthy points:

(a) The MK recognized that the massive dissemination of data and the ease of telecommunication, in both cyberspace and the real world, has raised concerns over the protection of the constitutional right of privacy.

(b) The MK agreed with the Petitioners that high-risk data processing should be subject to a higher standard of supervision.

(c) Regarding the cumulative formulation of Article 53 (1), the MK held that it fails to ensure the protection of individual rights guaranteed under Article 28G (1) of the Constitution.

On the basis of these points, the MK granted the Petitioners' lawsuit in full.

C. Implications of Decision 151

Following Decision 151, the threshold for appointing a DPO under Article 53 (1) of the PDP Law has been significantly lowered. An organization now triggers the mandatory DPO requirement by meeting any one of the three criteria, rather than all three. This shift reflects the broader policy objective of enhancing oversight and protecting individuals in high-risk data processing activities.

Many companies, especially those handling large volumes of personal data, may now need to appoint a DPO. This does not necessarily require a new hire, as an existing staff member with the necessary skills can serve in the role, though companies lacking in-house expertise may need appoint a qualified professional.

.....

Click the "download file" button to read the PDF version.

If you have any questions, please contact:

1. Reagan Roy Teguh, Partner – reagan.teguh@makarim.com
2. Dante Deva Daniswara, Associate - dante.daniswara@makarim.com

© 2007 The McGraw-Hill Companies. All rights reserved. This publication is protected by copyright. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without prior written permission from The McGraw-Hill Companies, Inc.