

Digital Trust NewsFlash

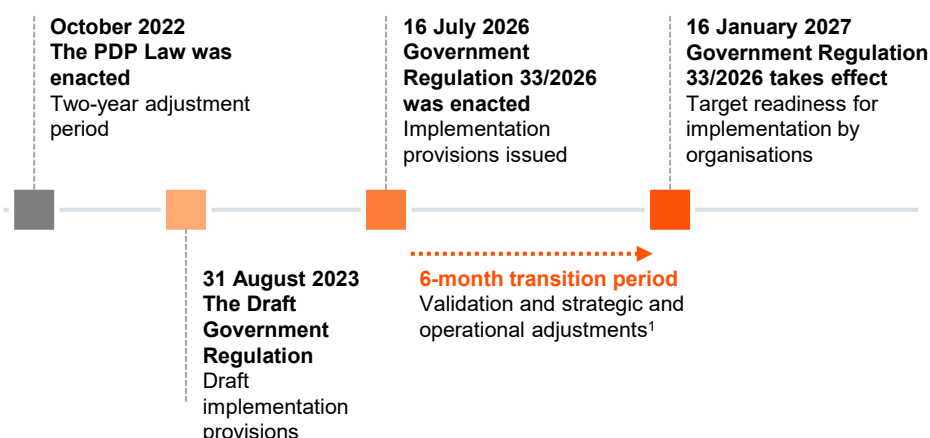
September 2026 / No. 12

Government Regulation 33/2026 on Personal Data Protection: key changes and action points

A. Background

On 16 July 2026, the Indonesian Government issued Government Regulation No. 33 of 2026 on the Implementation of Law No. 27 of 2022 on Personal Data Protection ("**Government Regulation 33/2026**"). Government Regulation 33/2026 will take effect on 16 January 2027. Although largely aligned with the previously circulated draft regulation ("**Draft Government Regulation**"), Government Regulation 33/2026 introduces important refinements and provides a clearer framework for regulatory supervision, compliance, and enforcement.

Landscape and timeline of the Personal data protection (PDP) regulatory framework



¹) Government Regulation 33/2026 generally maintains the main structure of the Draft Government Regulation but does not adopt it identically. In comparison with the Draft Government Regulation, Government Regulation 33/2026 amends several provisions, while some implementing provisions will be further regulated by the Personal Data Protection Authority ("**PDP Authority**"). In general, organisations can use the compliance framework previously developed based on the Draft Government Regulation as a starting point, but **should validate and adjust it in line with the requirements of Government Regulation 33/2026 throughout the transition period.**

Government Regulation 33/2026 introduces significant operational, procedural, and enforcement requirements, while certain aspects remain dependent on the establishment of the PDP Authority and further implementing instruments. In this regard, as of the date of this publication, the PDP Authority had not yet been established, which remains a significant outstanding issue for the implementation and enforcement of Government Regulation 33/2026. The previous provisions under the Draft Government Regulation may be adopted as a starting point for organisations to establish their initial compliance frameworks, however it should be further validated and updated to reflect the requirements introduced under the Government Regulation 33/2026. This NewsFlash highlights the key changes.

B. Key changes to note

Government Regulation 33/2026 retains the overall framework of the Draft Government Regulation but refines provisions that directly affect how personal data protection programmes are designed and run. The headline changes are below.

1. Six-month transition period

The Draft Government Regulation contemplated immediate effectiveness. Government Regulation 33/2026 instead gives organisations until 16 January 2027 to comply with the regulation.

2. A stricter consent standard applies

The Draft Government Regulation did not expressly require consent to be unambiguous. Under Government Regulation 33/2026, consent must be unambiguous, and consent bundled with acceptance of general terms and conditions may be considered ambiguous.

3. Privacy notice requirements are streamlined, but important details remain

Government Regulation 33/2026 streamlines the minimum information required in privacy notices, while several detailed items remain reflected in the elucidation. It also adds new mandatory disclosures where companies jointly control the same personal data, covering the controllers involved, how their processing purposes relate to one another, the manner of processing, and the jointly appointed contact point.

4. Exoneration clauses are prohibited in privacy notices

Government Regulation 33/2026 now prohibits exoneration clauses in personal data protection notices generally, across all legal bases.

5. Contracts used as a legal basis face stricter requirements

Government Regulation 33/2026 expands the minimum content for contracts to be relied on as a legal basis. A contract that fails to fulfil those requirements can no longer be used as a legal basis for processing.

6. Updated criteria for appointing a personal data protection officer

The Draft Government Regulation applied the data protection officer (DPO) conditions cumulatively. Following Constitutional Court Decision No. 151/PUU-XXII/2024, Government Regulation 33/2026 treats the conditions as alternatives, so meeting any one of the conditions will trigger the obligation.

7. Audit obligations move from discretionary to mandatory

Under the Draft Government Regulation, controllers were permitted, but not required, to conduct internal and external audits of their personal data protection practices. Government Regulation 33/2026 now requires controllers to carry out both internal and external audits. The minimum scope, methodology, and frequency are not specified and may be addressed in future PDP Authority policies.

8. Internal policies will depend on future PDP Authority guidelines, except for data retention

Companies must still maintain an internal policy on personal data processing, but its detailed content will follow future PDP Authority policies rather than the prescriptive list under the Draft Government Regulation. Separately, Government Regulation 33/2026 requires controllers to establish a documented retention policy along with its minimum content.

9. Controllers' records of processing activities (ROPA) must now capture data transfers

Controllers must now maintain their own transfer records and make them available for audit and supervisory purposes, extending a requirement that previously applied only to processors under the Draft Government Regulation.

10. Personal data protection failures now extend beyond unauthorised disclosure

Government Regulation 33/2026 now captures unauthorised alteration, corruption, destruction, loss, and loss of access as personal data protection failures. Ransomware, accidental deletion and system failures may now be in scope even where no data was disclosed.

11. A different mechanism applies to children's data subject rights

Government Regulation 33/2026 allows either a child or the parent or guardian to submit a data subject rights request. Where a child submits directly, the controller must assess the child's capacity to understand the right being exercised. The elucidation nonetheless confirms that exercising rights relating to the processing of a child's personal data still requires parental or guardian consent.

12. New data-processing requirements apply to corporate actions

Under Government Regulation 33/2026, in the event of a corporate action involving the transfer of personal data between controllers, controllers must assess the impact on data subject rights and controller obligations, update the data protection impact assessment (DPIA) where required, and implement technical measures for the transfer. Until the corporate action is deemed completed under the prevailing laws, the transferring and receiving controllers are deemed Joint Controllers.





C. What should your organisation do next?



1. Run a focused **gap assessment** of current practices against Government Regulation 33/2026, covering the changes above and the wider requirements not addressed in this NewsFlash.



2. Strengthen **consent mechanisms and legal-basis documentation**, presenting consent separately from general terms and conditions and supporting it with adequate evidence.



3. Update **contracts relied on as a legal basis** against Government Regulation 33/2026 minimum content, and revisit processor and third-party agreements for oversight, documentation, and audit rights.



4. Establish a **mandatory internal and external audit programme**, and ensure **ROPA** captures relevant domestic and cross-border personal data transfers and can be produced promptly.



5. Expand incident management to the broader concept of a **Personal Data Protection Failure**, and reassess **DPO appointment criteria** now that the conditions are alternative.



6. Track further **PDP Authority guidance** where Government Regulation 33/2026 leaves technical details open, and maintain a process for updating the compliance framework as such guidance is issued.



7. Complete readiness before **16 January 2027**, strengthening governance and maintaining documentation that demonstrates compliance for supervisory purposes.

For more information, please contact our PwC Indonesia team below:



Subianto

Broader Assurance Services Leader
Chief Digital & Technology Officer
subianto.subianto@pwc.com



Indra Allen

Legal Partner
indra.allen@pwc.com



Richard Ticoalu

Data, AI and Risk Partner
richard.ticoalu@pwc.com



Hengky Antony

Data & Analytics Director
hengky.antony@pwc.com



Marcello Dwianto

Senior Manager
marcello.dwianto@pwc.com



Sultan Buruni

Legal Senior Managing
Associate
sultan.buruni@pwc.com



Putu Putra

Legal Managing Associate
putu.putra@pwc.com



Ivan Kirsten

Manager
ivan.k.kirsten@pwc.com

www.pwc.com/id



PwC Indonesia



@PwC_Indonesia

This publication has been prepared for general guidance on matters of interest only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC Indonesia, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

PwC Indonesia is comprised of KAP Rintis, Jumadi, Rianto & Rekan, PwC Tax Indonesia, PwC Legal Indonesia, PT PwC Advis Indonesia and PT PricewaterhouseCoopers Consulting Indonesia, each of which is a separate legal entity and all of which together constitute the Indonesian member firms of the PwC global network, which is collectively referred to as PwC Indonesia.

© 2026 PwC. All rights reserved.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see <http://www.pwc.com/structure> for further details.