STRATEGI KEPATUHAN & TATA KELOLA KORPORASI

Jawaban Strategis atas Implikasi & Kesiapan Perusahaan Menghadapi PP No. 33 Tahun 2026 tentang Pelindungan Data Pribadi

Analisis Kesiapan, Kesenjangan Implementasi, Peta Jalan Risk-Based, dan Adopsi Teknologi PDP

EXECUTIVE ADVISORY BRIEFING | Kerangka Acuan UU No. 27/2022 & PP No. 33/2026 | Model Tata Kelola DPOaaS

RESPONS STRATEGIS PP 33 TAHUN 2026

PP 33/2026 Menuntut Transisi dari Kepatuhan Administratif Menuju Akuntabilitas Operasional

1. Kepastian vs Kompleksitas

PP 33/2026 memberikan kepastian parameter hukum pemrosesan data, namun meningkatkan kompleksitas operasional dengan sanksi denda administratif hingga 2% pendapatan tahunan.

2. Kesenjangan Utama

Kesenjangan terbesar berada pada operasional pemenuhan hak subjek data (DSR SLA 3x24h), tata kelola vendor/Prosesor, dan penanganan insiden kebocoran data 72 jam.

3. Pendekatan Risk-Based

Pendekatan bertahap berbasis risiko (Phased Risk-Based Approach) adalah pilihan paling realistis dibanding merombak total sistem sekaligus.

4. Otomatisasi & DPOaaS

Pemanfaatan teknologi otomatisasi (DSR, RoPA, SIEM) dan ekosistem DPO as a Service (DPOaaS) mempercepat tingkat kematangan kepatuhan perusahaan.

PP 33/2026 Mendorong Kesiapan Melalui Kepastian Hukum Sekaligus Menghadirkan Tantangan Baru

SISI KEPASTIAN HUKUM (DORONGAN KESIAPAN)

- **Parameter Lawful Basis Jelas**:
  Mempertegas 6 dasar pemrosesan data (persetujuan eksplisit, perjanjian, kewajiban hukum, kepentingan vital, tugas publik, & legitimate interest) [Pasal 30].
- **Standar Klausul Kontrak (DPA)**:
  Kepastian rumusan perjanjian wajib antara Pengendali dan Prosesor Data Pribadi [Pasal 14].
- **Batas & Aturan Perekaman RoPA**:
  Panduan konkret 13 elemen wajib perekaman aktivitas pemrosesan data [Pasal 74].
- **Kejelasan Tata Cara Sanksi & Hak**:
  Ketentuan pasti mengenai mekanisme ganti rugi dan pengawasan oleh Lembaga PDP [Pasal 105, 184].

SISI KOMPLEKSITAS & TANTANGAN BARU

- **Sanksi Denda Maksimal 2%:**
  Ancaman denda administratif hingga 2% dari pendapatan/penerimaan tahunan korporasi [Pasal 185].
- **SLA Ketat Penanganan Kebocoran**:
  Wajib menyampaikan notifikasi tertulis kebocoran data maksimal 3x24 jam kepada Otoritas & Subjek Data [Pasal 114].
- **Mandat DPIA Berisiko Tinggi**:
  Kewajiban menyusun Penilaian Dampak PDP secara sistematis sebelum memproses data spesifik/skala besar/AI [Pasal 120-121].
- **Tanggung Jawab & Pengawasan**:
  Pengendali bertanggung jawab atas seluruh tindakan Prosesor data di bawah kendalinya [Pasal 13, 126].

Kesenjangan Signifikan Terjadi pada Tiga Area Operasional Kritis Korporasi

Area 1: Operasional Hak Subjek Data (DSR)

Kesenjangan SLA 3x24 Jam

- Wajib menyediakan kanal permohonan DSR yang mudah diakses dan diverifikasi secara proporsional [Pasal 21, 25].
- Kewajiban penundaan/pembatasan pemrosesan dalam waktu maksimal 3x24 jam [Pasal 99, 103].
- **Tantangan**: Mayoritas perusahaan belum memiliki otomatisasi sistem ticketing DSR dan pencabutan konsen.

Area 2: Pengawasan Vendor & Pihak Ketiga

Tanggung Jawab Pengendali

- Penunjukan Prosesor wajib diikat perjanjian klausul PDP (DPA) terperinci [Pasal 14].
- Pengendali tetap bertanggung jawab atas pemrosesan data oleh Prosesor [Pasal 13(3)].
- **Tantangan**: Ketiadaan inventarisasi vendor, audit berkala Prosesor, dan Standard Contractual Clauses (SCC).

Area 3: Respons Insiden & Notifikasi

Batas Waktu Notifikasi 3 Hari Kerja

- Notifikasi tertulis kebocoran data wajib disampaikan paling lambat 3x24 jam [Pasal 114].
- Wajib menyusun dokumen analisis dampak, root cause, dan mitigasi pemulihan [Pasal 116].
- **Tantangan**: Integrasi SIEM/DLP yang minim dan ketiadaan simulation playbook penanganan insiden siber.

RESPONS STRATEGIS PP 33 TAHUN 2026

Pencapaian Kepatuhan Realistis Melalui Fleksibilitas Struktur Organisasi PDP & DPOaaS

REALITAS KEMATANGAAN & TANTANGAN SUMBER DAYA

- **Heterogenitas Kapasitas**: UMKM, BUMN, dan Multi-Nasional memiliki tingkat kematangan sistem TIK dan anggaran yang sangat timpang.
- **Keterbatasan Talenta DPO/PPDP**: Kelangkaan praktisi terampil yang menguasai kombinasi hukum, IT, dan manajemen risiko privasi.
- **Kompleksitas Biaya & Waktu**: Tidak realistis bagi seluruh perusahaan untuk memenuhi 100% ketentuan PP sekaligus dalam waktu singkat tanpa mengganggu operasional bisnis.
- **Risiko Over-Engineering**: Pemaksaan solusi mahal yang tidak sebanding dengan tingkat risiko nyata pemrosesan data.

SOLUSI REGULASI: DPO AS A SERVICE (DPOaaS)

- **Landasan Hukum Eksternalisasi DPO:** UU PDP Pasal 53(3) & PP 33/2026 Pasal 144(2) memperbolehkan PPDP berasal dari luar Pengendali/Prosesor Data.
- **Fleksibilitas Struktur DPOaaS:** Perusahaan dapat memanfaatkan model Fractional DPO, Virtual DPO, Shared DPO (Holding-Anak Usaha), atau Co-Sourced DPO**.**
- **Efisiensi Biaya (Cost-Effective):** Skema Monthly Retainer atau Advisory Note menghemat biaya tetap SDM internal sambil tetap menjaga independensi pelaporan ke Direksi [Pasal 146].
- **Skalabilitas Bertahap:** Mengalokasikan sumber daya eksternal fokus pada area berisiko tinggi (RoPA & DPIA) sesuai kapasitas investasi.

RESPONS STRATEGIS PP 33 TAHUN 2026

Pendekatan Bertahap Berbasis Risiko (Phased Risk-Based Approach) Adalah Strategi Terbaik

FASE 1: DIAGNOSTIK & ROPA
Bulan 1 - 3

- Pemetaan aliran data (Data Mapping).
- Penyusunan Perekaman RoPA [Pasal 74].
- Identifikasi pemrosesan berisiko tinggi.

FASE 2: TATA KELOLA & DPA
Bulan 3 - 6

- Penerbitan Kebijakan PDP Internal [Pasal 28].
- Penunjukan DPO/PPDP & DPA Vendor [Pasal 14, 142].
- Pembaruan Privacy Notice [Pasal 62].

FASE 3: OPERASIONALISASI
Bulan 6 - 9

- Pelaksanaan DPIA berisiko tinggi [Pasal 120].
- Portal DSR & SLA Penundaan 3x24h [Pasal 99].
- Simulasi Incident Response 72h [Pasal 114].

FASE 4: AUDIT & OPTIMALISASI
Bulan 9 - 12+

- Audit internal/eksternal PDP [Pasal 138].
- Penerapan teknologi PET & Enkripsi [Pasal 123].
- Sertifikasi ISO 27701 & Tinjauan Berkala.

RESPONS STRATEGIS PP 33 TAHUN 2026

Tiga Langkah Paling Mendesak Menjelang Pemberlakuan PP No. 33 Tahun 2026

LANGKAH 1

Pembentukan Task Force & Penunjukan DPO/PPDP

Membentuk tim lintas fungsi (Risk, Legal, IT, HR, Ops) dan menetapkan DPO/PPDP (internal atau DPOaaS) dengan akses pelaporan langsung ke Direksi [Pasal 142, 146].

LANGKAH 2

Penyusunan Perekaman RoPA & Pemetaan Aliran Data

Menyusun Perekaman Kegiatan Pemrosesan Data Pribadi (RoPA) secara terstruktur [Pasal 74] sebagai kompas utama identifikasi *lawful basis* dan *high-risk processing*.

LANGKAH 3

Penetapan SLA DSR 3x24 Jam & Playbook Insiden 72 Jam

Menyusun Kebijakan Internal, kanal DSR ber-SLA 3x24 jam [Pasal 99], serta **Incident Response Plan** untuk memenuhi kewajiban notifikasi kebocoran data 3x24 jam [Pasal 114].

MEMASTIKAN IMPLEMENTASI OPERASIONAL: Dilakukan melalui pengujian berkala (Tabletop Exercise insiden), indikator KPI bulanan/kuartalan DPO, serta evaluasi kepatuhan vendor [Pasal 126, 138].

RESPONS STRATEGIS PP 33 TAHUN 2026

Otomatisasi Teknologi Berfokus pada Proses Berulang dengan SLA Ketat

Proses Berulang Utama	Kebutuhan Otomatisasi Teknologi	Manfaat Efektivitas & Efisiensi
Manajemen Hak Subjek Data (DSR Portal)	Automated DSR Ticketing & Consent Log Management untuk pemenuhan SLA penundaan/pembatasan 3x24 jam [Pasal 99].	Mencegah keterlambatan respon, meminimalisasi human error, dan menyediakan audit trail otomatis.
Data Discovery & RoPA Automation	Pemetaan data sensitif otomatis di database/cloud serta pemutakhiran terpusat Perekaman RoPA [Pasal 74].	Visibilitas real-time atas aliran data tanpa harus mengganggu aktivitas kerja rutin unit operasional.
Security Control & Incident Monitoring	Pengintegrasian DLP, Enkripsi Data, SIEM/SOC, dan Privacy Threat Hunting untuk deteksi dini insiden [Pasal 123].	Memastikan pemenuhan SLA notifikasi kebocoran 3x24 jam [Pasal 114] dan mencegah insiden berulang.

MEMASTIKAN EFEKTIVITAS INVESTASI TEKNOLOGI (ROI):

1. Hindari produk terisolasi (siloed tools); utamakan modul yang terintegrasi dengan infrastruktur siber existing (ISO 27001/27701).
2. Evaluasi berbasis risiko (melihat hasil DPIA) [Pasal 124] agar biaya implementasi sebanding dengan potensi nilai dan dampak risiko bisnis.

KESIMPULAN STRATEGIS

Transformasi PDP Adalah Investasi Keberlanjutan Bisnis dan Kepercayaan Pemangku Kepentingan

01. Kepastian & Tata Kelola

PP 33/2026 mengubah tata kelola PDP dari tugas teknis IT menjadi pertanggungjawaban strategis korporasi (Corporate Governance).

02. Phased Risk-Based Road

Pelaksanaan bertahap fokus pada RoPA, DPIA berisiko tinggi, dan fleksibilitas DPOaaS untuk optimasi biaya dan sumber daya.

03. Integrasi & Otomatisasi

Investasi teknologi pada otomatisasi DSR SLA 3x24h dan insiden 72h melindungi reputasi serta mencegah denda 2% pendapatan.

REKOMENDASI AKHIR: Segera sahkan Task Force PDP, mulailah penyusunan Perekaman RoPA, dan evaluasi pengadopsian DPOaaS serta modul otomatisasi DSR untuk menjamin kepatuhan operasional sebelum pemeriksaan Otoritas.