Ringkasan Kebijakan No. 1

Dari Aturan ke Perlindungan: Menutup Kesenjangan Implementasi UU Pelindungan Data Pribadi di Indonesia

oleh Kirana Aisyah dan Audy Maharani Sagita



Ringkasan Eksekutif

Indonesia telah memiliki kerangka hukum pelindungan data pribadi yang relatif komprehensif melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU tersebut mengatur hak subjek data, kewajiban pengendali dan prosesor, sanksi, mekanisme transfer data lintas negara, serta pembentukan lembaga pengawas. Masa penyesuaiannya telah berakhir pada 17 Oktober 2024. Karena itu, tantangan utama pelindungan data pribadi di Indonesia kini bergeser dari pembentukan kerangka hukum menuju bagaimana memastikan aturan tersebut dapat diimplementasikan dan ditegakkan secara efektif.

Ringkasan kebijakan ini mengintegrasikan analisis hukum dan kebijakan komparatif UU PDP–GDPR, survei Safe Nusa terhadap 209 responden, serta tujuh wawancara semiterstruktur dengan regulator, akademisi, dan praktisi. Ketiga sumber bukti digunakan secara triangulatif untuk membandingkan apa yang diatur secara normatif, apa yang diketahui dan dialami responden, serta bagaimana para ahli menjelaskan persoalan implementasinya.

"**83,3%** responden belum mengetahui secara tepat status lembaga pengawas PDP; hanya **33,5%** menyatakan percaya bahwa lembaga pemerintah melindungi data pribadi mereka; **73,2%** mendukung pengawasan PDP oleh **otoritas independen**; dan **96,2%** menginginkan **penegakan hukum yang lebih kuat**." Wawancara juga menunjukkan bahwa kepatuhan dalam beberapa kasus masih berhenti pada dokumen atau "***on paper***", sementara survei menemukan kesenjangan antara persepsi pemahaman terhadap UU PDP dan pengetahuan faktual.

Perbandingan dengan GDPR memperlihatkan bahwa kesenjangan Indonesia tidak semata-mata terletak pada substansi hak yang diberikan. UU PDP telah memiliki banyak elemen yang sejalan secara prinsip dengan GDPR. Perbedaan yang lebih relevan terdapat pada arsitektur implementasi yang menghubungkan norma hukum dengan institusi pengawas, penegakan, kepatuhan organisasi, mekanisme pemulihan, dan kemampuan masyarakat menggunakan haknya.

Oleh karena itu, ringkasan kebijakan ini merekomendasikan **lima prioritas,** yaitu:

1. Mengoperasionalkan otoritas pengawas PDP dengan independensi fungsional, kewenangan, sumber daya, dan mekanisme akuntabilitas yang jelas
2. Membangun arsitektur koordinasi penegakan antara otoritas PDP dan regulator sektoral
3. Menyediakan mekanisme pengaduan, investigasi, dan pemulihan yang sederhana serta mudah digunakan masyarakat
4. Menggeser literasi PDP dari sekadar *awareness* menuju pengetahuan yang dapat diukur dan kemampuan praktis menggunakan hak
5. Mendorong kepatuhan berbasis risiko dan *privacy by design*, termasuk pengembangan AI dan teknologi baru

Dengan demikian, agenda berikutnya bagi Indonesia bukan sekadar menambah aturan, tetapi menutup kesenjangan implementasi antara hak yang tersedia di atas kertas dan perlindungan yang benar-benar dapat dirasakan masyarakat.

Latar Belakang: Dari Pembentukan UU Menuju Tantangan Implementasi

Transformasi digital telah meningkatkan volume dan intensitas pengumpulan, pemrosesan, dan pertukaran data pribadi dalam berbagai aktivitas masyarakat, mulai dari layanan keuangan, perdagangan elektronik, media sosial, hingga pelayanan publik. Perluasan aktivitas digital tersebut membawa manfaat ekonomi dan sosial, tetapi pada saat yang sama memperbesar paparan masyarakat terhadap penyalahgunaan data, pelanggaran privasi, dan kebocoran informasi.

90,0%	**pernah mengalami setidaknya satu dari empat jenis insiden keamanan digital atau privasi yang ditanyakan dalam survei**
38,3%	**pernah menerima pesan *phishing* yang memuat data pribadi**
47,8%	**menyatakan salah satu akun daring pernah diakses tanpa izin**
47,4%	**pernah menerima OTP yang tidak diminta**

Temuan tersebut tidak berarti bahwa 90% responden mengalami pelanggaran UU PDP atau bahwa seluruh insiden berasal dari kebocoran data. Temuan lebih tepat dibaca sebagai indikasi luasnya paparan responden terhadap risiko yang berkaitan dengan akun, identitas, dan data pribadi. Pembedaan tersebut penting karena risiko keamanan akun, penipuan digital, dan pelanggaran kewajiban pelindungan data merupakan kategori yang dapat saling berkaitan tetapi tidak identik secara hukum. (Safe Nusa, 2026)

Indonesia Telah Memiliki Kerangka Hukum melalui UU PDP

Indonesia mengambil langkah penting dengan mengundangkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi pada 17 Oktober 2022. Sebelum UU PDP, pengaturan mengenai data pribadi tersebar dalam berbagai regulasi sektoral. Kehadiran UU PDP karena itu menandai perubahan penting menuju kerangka hukum nasional yang lebih komprehensif mengenai pemrosesan dan pelindungan data pribadi. Pada 2026, pemerintah juga menerbitkan Peraturan Pemerintah Nomor 33 Tahun 2026 sebagai aturan pelaksanaan UU PDP, yang memperinci sejumlah aspek operasional pelindungan data pribadi dan mulai berlaku pada 16 Januari 2027. (Republik Indonesia, 2022; Republik Indonesia, 2026; Simbolon & Juwono, 2022; Razi dkk., 2024)

Terbitnya aturan pelaksanaan tersebut memperjelas kerangka implementasi, tetapi tidak otomatis menyelesaikan seluruh persoalan. Pertanyaan yang semakin penting adalah apakah hak, kewajiban, standar kepatuhan, pengawasan, dan mekanisme penegakan yang telah ditetapkan dapat benar-benar bekerja dalam praktik.

Metodologi

Ringkasan kebijakan ini menggunakan pendekatan *mixed-methods* dengan mengintegrasikan bukti kuantitatif dan kualitatif untuk memperoleh pemahaman yang lebih komprehensif mengenai implementasi pelindungan data pribadi di Indonesia. Triangulasi dilakukan terhadap tiga sumber bukti: analisis hukum dan kebijakan komparatif; survei publik* terhadap 209 responden; dan wawancara semiterstruktur dengan tujuh ahli dan praktisi.

1. **Analisis hukum dan kebijakan komparatif**

   Membandingkan UU PDP dan GDPR untuk mengidentifikasi persamaan, perbedaan, kesenjangan implementasi, dan praktik kelembagaan yang dapat menjadi pembelajaran bagi Indonesia.

2. **Survei publik**

   Survei pelindungan data pribadi Safe Nusa dilaksanakan pada 13–21 Juli 2026 dan melibatkan 209 responden berusia 15–30 tahun. Instrumen mencakup pengalaman risiko, pengetahuan, kepercayaan, perilaku, desain kelembagaan, dan preferensi kebijakan.

3. **Wawancara ahli**

   Tujuh wawancara semiterstruktur dilakukan pada Agustus–September 2026 dengan perspektif regulator/pemerintah, akademisi hukum, hukum dan teknologi, tata kelola digital, serta *governance, risk, and compliance* (GRC).

Rekomendasi kebijakan tidak diturunkan dari satu indikator survei atau satu pernyataan narasumber secara terpisah. Rekomendasi dikembangkan dengan mempertimbangkan keterkaitan antara kerangka hukum, pola empiris dalam survei, perspektif ahli, dan pembelajaran komparatif.

Narasumber Wawancara Ahli

Narasumber mewakili perspektif regulator/pemerintah, akademisi hukum, hukum dan teknologi, tata kelola digital, serta *governance, risk, and compliance* (GRC). Keragaman tersebut digunakan untuk membandingkan bagaimana persoalan yang sama dipahami dari sudut pandang regulator, akademisi, dan praktisi implementasi.

Narasumber	Institusi dan Latar Belakang	Perspektif
Bapak Syahraki Syahrir, S.E., Ak., M.M., CA, CISA, CISM, CDPSE, GRCP, GRCA	CEO Veda Praxis; lebih dari 20 tahun berkecimpung dalam konsultasi *governance, risk management*, dan *compliance*; mantan Presiden ISACA Indonesia	*Digital governance*, GRC, kematangan organisasi, implementasi UU PDP dan kepercayaan
Ibu Imelda Cardiana Sirait, GRCP, IRMP, IDPP, IAAP, ITGRC	Partner dan Head of PDP *Center of Excellence*, Veda Praxis; berlatar belakang audit, *risk management*, dan pendampingan implementasi PDP lintas industri	Kepatuhan organisasi, *privacy maturity*, DPO, *privacy by design*, dan implementasi PDP
Ibu Rindy, S.Kom., M.T.I., JNCIS, CEH, ECSA, LA/A ISO 27001, DPO	Kementerian Komunikasi dan Digital; Ketua Tim Pengawasan Kepatuhan Ruang Digital; memiliki pengalaman pada keamanan informasi, keamanan data, dan PDP	Perspektif regulator, pengawasan kepatuhan, penegakan, pengaduan dan literasi
Ibu Prof. Dr. Sinta Dewi Rosadi, S.H., LL.M.	Akademisi hukum Universitas Padjadjaran dengan fokus pada pelindungan data pribadi	Kerangka hukum PDP, independensi dan desain lembaga pengawas, hak subjek data dan penegakan
Bapak Dr. Wahyu Yun Santoso, S.H., M.Hum., LL.M.	Akademisi Fakultas Hukum Universitas Gadjah Mada; Pusat Kajian Hukum dan Teknologi	Hukum dan teknologi, regulasi pelaksana, desain kelembagaan dan implementasi

*Survei menggunakan sampel sukarela dan non-probabilistik. Karena probabilitas setiap anggota populasi untuk masuk ke dalam sampel tidak diketahui, persentase survei diinterpretasikan sebagai gambaran pola pada 209 responden, bukan sebagai estimasi prevalensi pada seluruh masyarakat Indonesia.

Narasumber	Institusi dan Latar Belakang	Perspektif
Bapak Faiz Rahman, S.H., LL.M.	Akademisi Hukum Tata Negara Fakultas Hukum Universitas Gadjah Mada; penelitian mengenai kepentingan umum dalam pelindungan data pribadi	Kepentingan umum, kepentingan negara, privasi, hak subjek data dan desain institusional
Bapak Dr. Bambang Pratama, S.H., M.H.	Akademisi dan peneliti hukum siber dengan kajian mengenai hukum teknologi, AI dan pelindungan data pribadi	Hukum siber, AI, perkembangan teknologi, desain regulasi dan respons kelembagaan

Sumber: Safe Nusa (2026), transkrip wawancara ahli, Agustus–September 2026.

UU PDP dan GDPR: Sama dalam Prinsip, Berbeda dalam Implementasi

Pengesahan UU PDP membawa kerangka pelindungan data Indonesia lebih dekat dengan prinsip-prinsip yang telah berkembang dalam General Data Protection Regulation (GDPR) Uni Eropa. Kesamaan tersebut terlihat dalam pengakuan hak subjek data, kewajiban pengendali dan prosesor, penggunaan dasar hukum pemrosesan, prinsip akuntabilitas, kewajiban notifikasi kegagalan pelindungan data, hingga pengaturan transfer data lintas negara. Kesamaan tersebut tidak berarti kedua rezim identik. Perbedaan penting justru muncul ketika regulasi dilihat sebagai sistem tata kelola, bukan sekadar kumpulan hak dan kewajiban. (Republik Indonesia, 2022; European Parliament & Council of the European Union, 2016; Simbolon & Juwono, 2022)

Dimensi	Perbandingan UU PDP-GDPR	Implikasi bagi Indonesia
Hak dan dasar pemrosesan	Keduanya mengakui hak subjek data dan menggunakan beberapa dasar pemrosesan, bukan hanya persetujuan. UU PDP mengatur hak seperti akses, koreksi, penghapusan, penarikan persetujuan, keberatan atas keputusan otomatis, ganti rugi, dan portabilitas.	Gap utama bukan lagi pada daftar hak, tetapi pada kemampuan warga menggunakan hak serta kemampuan organisasi menentukan dan mendokumentasikan dasar pemrosesan yang tepat.
Akuntabilitas organisasi	UU PDP maupun GDPR menempatkan kewajiban pada pengendali dan prosesor data pribadi serta menggunakan prinsip akuntabilitas.	Kepatuhan perlu terlihat dalam praktik — misalnya pemetaan data, asesmen risiko, kontrol akses, DPO, respons insiden, dan *privacy by design* — bukan berhenti pada dokumen.
Notifikasi kegagalan pelindungan data	Keduanya menggunakan batas waktu sekitar 72 jam, meski pemicu dan penerima notifikasinya berbeda. UU PDP mewajibkan pemberitahuan kepada subjek data dan lembaga; GDPR terutama mewajibkan notifikasi kepada *supervisory authority* dan, dalam kondisi tertentu, data subject.	Efektivitas bergantung pada prosedur yang jelas: kapan insiden wajib dilaporkan, kepada siapa, informasi apa yang dibutuhkan, dan bagaimana tindak lanjutnya.
Otoritas pengawas	UU PDP mengamanatkan lembaga pengawas yang ditetapkan Presiden; GDPR mewajibkan satu atau lebih *supervisory authorities* yang menjalankan tugasnya secara independen.	Prioritas Indonesia adalah memastikan independensi fungsional, kewenangan yang jelas, sumber daya, akuntabilitas, dan hubungan kerja dengan regulator sektoral.
Penegakan dan pemulihan	Keduanya menyediakan sanksi dan mekanisme penegakan. GDPR memberi *supervisory authorities* kewenangan investigatif dan korektif yang luas, di samping mekanisme administratif dan yudisial.	Persoalan utamanya bukan sekadar adanya sanksi, melainkan apakah pengaduan, investigasi, tindakan korektif, dan mekanisme pemulihan dapat dijalankan secara konsisten dan mudah diakses.
Transfer data lintas negara	Keduanya menggunakan konsep kecukupan perlindungan (*adequacy*), langkah perlindungan tambahan (*safeguards*), dan mekanisme pengecualian tertentu untuk transfer data lintas negara.	Indonesia sudah memiliki kerangka substantif; tantangan berikutnya adalah membuat *assessment*, *safeguards*, dan mekanisme pengawasannya benar-benar operasional.
Literasi dan penggunaan hak	UU PDP menempatkan peningkatan kesadaran sebagai tujuan pelindungan data; GDPR juga memberi tugas kepada *supervisory authorities* untuk meningkatkan *public awareness* and *understanding.*	Literasi perlu diukur dari pengetahuan aktual dan kemampuan menggunakan hak—termasuk mengetahui jalur pengaduan—bukan hanya *exposure* atau jumlah peserta sosialisasi.

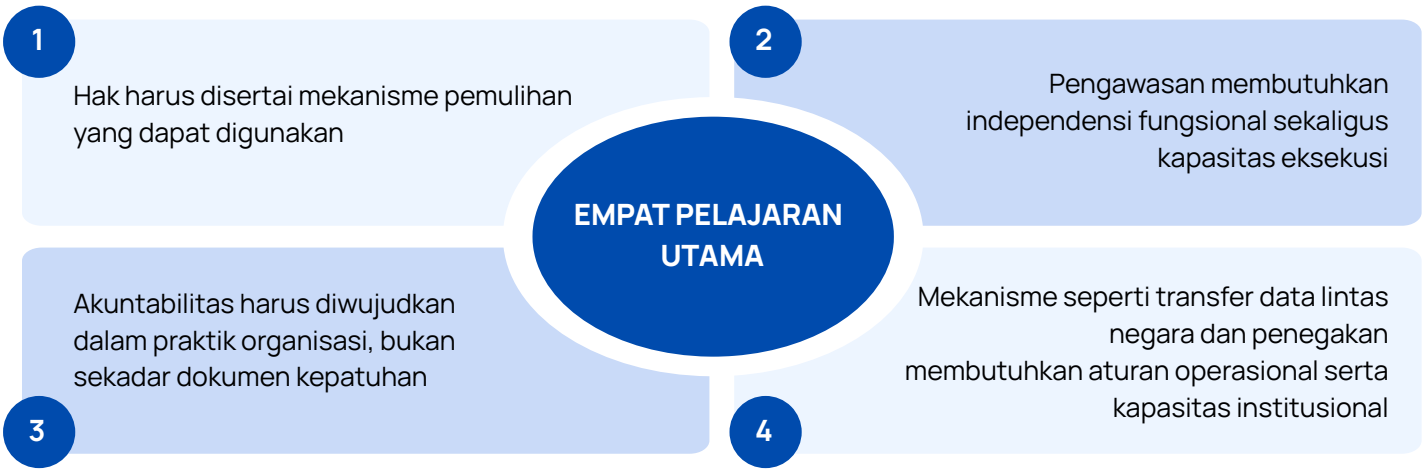
Sumber: diolah Safe Nusa berdasarkan UU No. 27 Tahun 2022, GDPR, literatur komparatif, dan wawancara ahli.

GDPR sebagai *Benchmark*, bukan *Blueprint*

Keseluruhan analisis menunjukkan bahwa UU PDP dan GDPR memiliki lebih banyak kesamaan pada tingkat prinsip dibandingkan yang sering diasumsikan. Hak subjek data, dasar pemrosesan, kewajiban pengendali dan prosesor, akuntabilitas, notifikasi kegagalan pelindungan data, sanksi, dan transfer data lintas negara telah memiliki landasan dalam UU PDP.

Temuan tujuh wawancara Safe Nusa memperkuat sekaligus memperumit gambaran tersebut. Ada kesamaan pandangan bahwa keberadaan undang-undang saja tidak cukup. Namun, para ahli tidak selalu menawarkan desain kelembagaan yang sama. Sebagian menekankan independensi struktural, sebagian menekankan independensi fungsional, sebagian menyoroti hubungan dengan regulator sektoral, sementara perspektif lain menempatkan kecepatan eksekusi sebagai hal yang penting.

Karena itu, pelajaran utama dari GDPR bukan bahwa Indonesia harus membangun replika institusi Eropa. Widiatedja dan Mishra (2023) menekankan pentingnya independensi organisasional dan fungsional otoritas PDP Indonesia, tetapi konteks nasional tetap menentukan bagaimana independensi tersebut diterjemahkan ke dalam struktur kelembagaan.



Dengan demikian, kesenjangan utama antara UU PDP dan GDPR tidak semata-mata berada pada jumlah hak atau ketatnya norma. Perbedaan yang lebih penting terletak pada arsitektur implementasi yang menghubungkan norma, institusi, penegakan, kepatuhan organisasi, dan kemampuan masyarakat menggunakan haknya.

Temuan Utama: Kesenjangan Implementasi UU PDP

Analisis terhadap survei Safe Nusa, tujuh wawancara semiterstruktur, serta literatur hukum dan kebijakan menunjukkan bahwa tantangan utama pelindungan data pribadi di Indonesia tidak lagi semata-mata terletak pada keberadaan regulasi. UU No. 27 Tahun 2022 telah menyediakan kerangka substantif mengenai hak subjek data, kewajiban pengendali dan prosesor, sanksi, serta kelembagaan. Namun, terdapat kesenjangan antara perlindungan yang tersedia secara normatif dan kemampuan sistem tata kelola untuk membuat perlindungan tersebut bekerja dalam praktik.

Temuan 1: Kesenjangan kelembagaan menjadi titik kritis implementasi UU PDP

UU PDP memberikan mandat yang luas kepada lembaga penyelenggara pelindungan data pribadi untuk melakukan pengawasan, menegakkan hukum administratif, menjatuhkan sanksi, menangani pengaduan, melakukan pemeriksaan, serta bekerja sama dengan otoritas pelindungan data negara lain. Namun, dimensi kelembagaan masih menjadi bagian yang belum sepenuhnya teroperasionalisasi. (Republik Indonesia, 2022; Kementerian Komunikasi dan Digital, 2026)

Hanya 16,7% responden Safe Nusa mengetahui secara tepat status lembaga pengawas PDP. Sebanyak 41,6% mengira lembaga tersebut sudah ada, sementara 41,6% menjawab tidak tahu. Dengan demikian, 83,3% responden belum mengetahui status kelembagaan yang sebenarnya. Temuan wawancara tidak menunjukkan konsensus mengenai satu bentuk organisasi tertentu; yang lebih konsisten adalah kebutuhan akan independensi dalam pengambilan keputusan, kewenangan yang jelas, kapasitas teknis dan sumber daya, serta kemampuan mengeksekusi keputusan secara efektif. (Safe Nusa, 2026)

Temuan 2: Penegakan lebih menentukan daripada sekadar keberadaan aturan

UU PDP telah menyediakan instrumen penegakan, termasuk sanksi administratif. Artinya, keberadaan norma sanksi dan keberadaan institusi yang mampu menjatuhkannya saling bergantung. Dari perspektif regulator, pengaduan masyarakat juga memperlihatkan persoalan praktis: warga tidak selalu mengetahui kepada siapa harus melapor, bukti apa yang diperlukan, atau bagaimana kasus akan diproses.

Survei Safe Nusa menemukan dukungan yang sangat tinggi terhadap penegakan yang lebih kuat: 96,2% responden menyatakan Indonesia membutuhkan penegakan hukum yang lebih kuat terhadap pelanggaran pelindungan data pribadi. Pengalaman GDPR juga menunjukkan bahwa independensi saja tidak cukup tanpa sumber daya dan kapasitas penegakan. (Safe Nusa, 2026; European Union Agency for Fundamental Rights, 2024; Baquero, 2025)

Temuan 3: Kepatuhan belum merata dan tidak boleh berhenti di atas kertas

Analisis wawancara menunjukkan bahwa kepatuhan organisasi merupakan salah satu tema paling dominan, tetapi juga sangat bervariasi menurut sektor dan tingkat kematangan organisasi. Ibu Imelda Cardiana Sirait, yang menjelaskan pengalamannya mendampingi hampir 50 perusahaan lintas sektor, merangkum salah satu pola kepatuhan: "Tapi kadang *on paper* aja ya, belum dilaksanakan."

Pernyataan tersebut membedakan *formal compliance* dari *substantive compliance*. Organisasi dapat memiliki kebijakan privasi, formulir persetujuan, SOP, atau dokumentasi PDP, tetapi keberadaan dokumen belum membuktikan bahwa prinsip PDP benar-benar tertanam dalam proses organisasi. Dari keseluruhan coding wawancara, kepatuhan substantif muncul dalam pembahasan mengenai pemetaan data, asesmen risiko, DPO, prosedur insiden, *privacy by design*, kontrol internal, keterlibatan pimpinan, dan tingkat kematangan tata kelola.

Implikasinya, pendekatan yang sama untuk semua organisasi berpotensi tidak efektif. Penegakan tetap membutuhkan standar minimum yang sama atas hak subjek data, tetapi cara organisasi mencapai dan membuktikan kepatuhan dapat mempertimbangkan tingkat risiko, skala pemrosesan, sensitivitas data, dan kematangan organisasi.

Temuan 4: Merasa paham tidak sama dengan benar-benar mengetahui

Salah satu temuan paling penting dari survei Safe Nusa adalah adanya ketidaksesuaian antara *perceived knowledge* dan *actual knowledge*. Di antara responden yang menyatakan merasa memahami UU PDP, 52,7% justru memberikan jawaban keliru mengenai status lembaga pengawas, dibandingkan 29,3% pada kelompok yang merasa kurang memahami. Temuan ini tidak berarti orang yang merasa memahami UU PDP secara umum memiliki pengetahuan lebih buruk, tetapi menunjukkan bahwa *self-assessment* tidak cukup digunakan sebagai proksi pengetahuan aktual. (Safe Nusa, 2026)

Temuan tersebut sejalan dengan penelitian literasi privasi yang menunjukkan bahwa *self-assessed privacy literacy* tidak selalu sejalan dengan *actual privacy literacy*. Program literasi karena itu perlu bergerak dari



(Ma & Chen, 2023)

Temuan 5: Kepercayaan publik merupakan bagian dari tata kelola PDP, bukan sekadar persoalan persepsi

Survei Safe Nusa menunjukkan perbedaan cukup besar dalam tingkat kepercayaan responden terhadap berbagai institusi yang mengelola data pribadi. Sebanyak 60,3% responden menyatakan percaya kepada perusahaan, 54,1% kepada platform digital, tetapi hanya 33,5% kepada lembaga pemerintah. Pada saat yang sama, 73,2% responden mendukung pengawasan PDP oleh otoritas independen. (Safe Nusa, 2026)

Bapak Syahraki Syahrir menempatkan kepercayaan sebagai elemen yang lebih luas dari digitalisasi: "*Trust* adalah mata uang pada era sekarang." Ia juga menekankan bahwa pemerintah sebagai pembuat aturan perlu memberikan teladan dalam pengelolaan data. Karena itu, kepercayaan tidak sebaiknya diperlakukan sebagai target komunikasi semata. Transparansi ketika terjadi insiden, akuntabilitas badan publik, konsistensi penegakan, mekanisme pengaduan yang kredibel, dan independensi pengawasan merupakan bagian dari infrastruktur kepercayaan itu sendiri.

Temuan 6: AI dan teknologi baru menguji kemampuan UU PDP untuk beradaptasi

AI, teknologi baru, dan *privacy by design* merupakan sejumlah tema yang muncul dalam tujuh wawancara ahli. Temuan tersebut tidak menunjukkan bahwa Indonesia membutuhkan rezim PDP yang sepenuhnya baru setiap kali teknologi baru muncul. Sebaliknya, wawancara cenderung menunjukkan pentingnya menerjemahkan prinsip PDP yang sudah ada ke dalam lingkungan teknologi yang berubah cepat.

AI, *big data*, *blockchain*, *profiling*, dan teknologi lain yang banyak bergantung pada data meningkatkan kompleksitas mengenai skala pemrosesan, inferensi data, transparansi, pembatasan tujuan, dan penghapusan data. Konsep data protection by design menyediakan salah satu jembatan antara prinsip hukum dan desain teknologi: perlindungan data ditempatkan dalam langkah teknis dan organisasional sejak awal, bukan hanya diperiksa setelah sistem selesai dibangun. (Veale, Binns, & Ausloos, 2018)

Kelembagaan menentukan siapa yang mengawasi dan menegakkan aturan; penegakan menentukan apakah hak memiliki konsekuensi nyata; kepatuhan organisasi menentukan apakah prinsip PDP masuk ke praktik sehari-hari; literasi menentukan apakah masyarakat dapat mengenali dan menggunakan hak; kepercayaan memengaruhi legitimasi tata kelola data; sementara AI dan teknologi baru menguji apakah keseluruhan sistem mampu beradaptasi.

Rekomendasi Kebijakan

Temuan penelitian menunjukkan bahwa penguatan implementasi UU PDP membutuhkan lebih dari penyempurnaan norma hukum. Prioritas kebijakan perlu diarahkan pada pembangunan kapasitas kelembagaan, mekanisme penegakan yang efektif, akses masyarakat terhadap pemulihan, peningkatan literasi yang terukur, serta kepatuhan organisasi yang mampu mengikuti perkembangan teknologi.

1 Operasionalkan otoritas pengawas PDP dengan independensi fungsional, kewenangan yang jelas, dan mekanisme akuntabilitas

Pembentukan dan operasionalisasi otoritas pengawas PDP perlu menjadi prioritas karena sejumlah fungsi penting dalam UU PDP bergantung pada keberadaan lembaga tersebut. Namun, pembentukan lembaga saja tidak cukup. Desain kelembagaan perlu menjamin independensi fungsional, yaitu kemampuan untuk melakukan investigasi, mengambil keputusan, dan menjatuhkan tindakan korektif tanpa intervensi terhadap penanganan kasus individual.

Temuan wawancara menunjukkan adanya perbedaan pandangan mengenai apakah independensi harus diwujudkan melalui pemisahan struktural penuh dari pemerintah. Meski demikian, terdapat titik temu yang lebih substantif: otoritas membutuhkan kewenangan yang jelas, kapasitas teknis, sumber daya yang memadai, kemampuan mengeksekusi keputusan, dan mekanisme akuntabilitas yang tidak mengurangi independensi pengawasannya.

Keberhasilan kebijakan sebaiknya tidak dinilai hanya dari terbentuknya lembaga, tetapi dari kesiapan operasionalnya: tersedianya personel dan anggaran, prosedur pemeriksaan, publikasi keputusan, waktu penyelesaian perkara, dan kemampuan menjalankan kewenangan secara konsisten.

2 Perjelas koordinasi penegakan antara otoritas PDP dan regulator sektoral

Pembentukan otoritas PDP tidak berarti regulator sektoral kehilangan relevansinya. Pemrosesan data terjadi dalam ekosistem yang telah memiliki struktur pengawasan sendiri. Persoalan muncul ketika pelanggaran data pribadi sekaligus bersinggungan dengan keamanan siber, perlindungan konsumen, regulasi sektoral, hukum pidana, atau kewajiban penyelenggara sistem elektronik.

Setelah otoritas PDP beroperasi, pemerintah perlu membangun protokol koordinasi antarlembaga yang menentukan pembagian fungsi antara otoritas PDP, Komdigi, OJK, aparat penegak hukum, dan regulator sektoral lainnya. Protokol perlu menjelaskan mekanisme rujukan kasus, pertukaran informasi, investigasi bersama, penentuan *lead authority*, serta penanganan perkara yang berada pada lebih dari satu rezim hukum.

3 Bangun mekanisme pengaduan dan pemulihan yang sederhana dan dapat digunakan masyarakat

Pengakuan hak dalam UU PDP hanya memiliki nilai praktis apabila subjek data dapat menggunakannya ketika terjadi pelanggaran. Karena itu, implementasi UU PDP perlu membangun hubungan yang jelas antara



Persoalannya bukan sekadar apakah masyarakat mengetahui bahwa mereka memiliki hak, tetapi apakah mereka memahami apa yang harus dilakukan ketika hak tersebut tidak dipenuhi.

Otoritas PDP perlu menyediakan satu pintu pengaduan yang mudah diakses, dengan bahasa yang sederhana dan prosedur yang dapat dipahami tanpa membutuhkan pengetahuan hukum yang mendalam. Sistem tersebut idealnya membantu pengguna mengidentifikasi jenis persoalan, pihak yang diduga bertanggung jawab, informasi atau bukti yang perlu diberikan, tahapan penanganan perkara, serta kemungkinan bentuk pemulihan. Apabila perkara berada di bawah kewenangan regulator atau aparat lain, sistem pengaduan perlu memiliki mekanisme rujukan yang jelas.

Indikator keberhasilan tidak hanya berupa jumlah kanal pengaduan yang dibentuk, tetapi juga tingkat penyelesaian pengaduan, waktu penanganan, aksesibilitas prosedur, bentuk pemulihan yang diberikan, dan pengalaman pengguna terhadap mekanisme tersebut.

4 Geser literasi PDP dari sekadar *awareness* ke pengetahuan yang terukur dan kemampuan menggunakan hak

Program literasi PDP perlu bergerak melampaui sosialisasi yang hanya bertujuan membuat masyarakat pernah mendengar mengenai UU PDP. Temuan survei Safe Nusa menunjukkan bahwa *self-reported awareness* tidak dapat dengan sendirinya digunakan sebagai ukuran pengetahuan aktual.

Pemerintah, otoritas PDP, lembaga pendidikan, dan organisasi masyarakat sipil perlu mengubah cara program literasi dirancang sekaligus dievaluasi. Materi edukasi sebaiknya berangkat dari situasi konkret, seperti apa yang dilakukan ketika akun diakses tanpa izin, ketika perusahaan menolak permintaan penghapusan data, ketika terjadi kebocoran, atau ketika seseorang ingin mengetahui data apa yang disimpan sebuah platform.

Jumlah peserta, jangkauan kampanye, atau persentase masyarakat yang mengaku memahami PDP dapat tetap dicatat, tetapi perlu dilengkapi dengan pertanyaan objektif dan simulasi yang mengukur apakah peserta benar-benar mengetahui hak dan mampu menentukan tindakan yang tepat.

5 Dorong kepatuhan berbasis risiko dan *privacy by design*, termasuk untuk AI dan teknologi baru

Implementasi UU PDP perlu menghindari pendekatan kepatuhan yang hanya menghasilkan dokumen. Kepatuhan substantif perlu terintegrasi ke dalam siklus pengelolaan data organisasi, mulai dari mengetahui data apa yang dikumpulkan dan untuk tujuan apa, menentukan dasar pemrosesan, melakukan pemetaan data dan asesmen risiko, membatasi akses, menyiapkan prosedur respons insiden, memastikan fungsi DPO berjalan ketika diwajibkan, hingga mengevaluasi risiko sebelum teknologi atau produk baru diluncurkan.

Standar perlindungan yang sama tidak berarti seluruh organisasi harus mengikuti proses kepatuhan yang identik. Organisasi memiliki profil risiko dan kapasitas yang berbeda. Karena itu, otoritas PDP bersama regulator sektoral perlu mengembangkan pendekatan pengawasan berbasis risiko, dengan prioritas lebih tinggi pada pemrosesan yang memiliki skala, sensitivitas, atau potensi dampak lebih besar terhadap hak individu.

AI dan teknologi baru perlu ditempatkan dalam kerangka yang sama. Karena perkembangan teknologi bergerak lebih cepat daripada perubahan undang-undang, pemerintah dan otoritas PDP perlu memiliki kapasitas untuk mengeluarkan panduan teknis yang adaptif, melakukan riset, melibatkan ahli, dan memperbarui interpretasi regulasi berdasarkan risiko yang muncul. *Privacy by design*, asesmen dampak pelindungan data, minimisasi data, transparansi, dan dokumentasi keputusan dapat menjadi instrumen untuk memungkinkan inovasi tanpa menempatkan perlindungan privasi sebagai pertimbangan setelah teknologi diluncurkan.

Keberhasilan rekomendasi ini sebaiknya tidak diukur dari jumlah organisasi yang memiliki dokumen kepatuhan, tetapi dari kematangan praktiknya: pelaksanaan asesmen risiko, pemetaan data, kesiapan respons insiden, penggunaan *privacy by design*, pelaksanaan asesmen dampak untuk pemrosesan berisiko tinggi, serta kemampuan organisasi menunjukkan bagaimana prinsip UU PDP diterapkan dalam sistem dan keputusan sehari-hari.

Arah Implementasi

Kelima rekomendasi tersebut perlu dipahami sebagai satu rangkaian, bukan lima agenda yang berdiri sendiri. Otoritas yang kuat tanpa mekanisme pengaduan akan membatasi akses masyarakat terhadap penegakan; pengaduan tanpa koordinasi regulator akan menghasilkan kebingungan kewenangan; penegakan tanpa panduan kepatuhan akan meningkatkan ketidakpastian organisasi; sementara hak tanpa literasi praktis akan sulit digunakan oleh masyarakat. Pada saat yang sama, perkembangan AI dan teknologi baru membuat keseluruhan sistem perlu mampu beradaptasi terhadap risiko yang terus berubah.

Rantai Implementasi



Karena itu, tujuan implementasi UU PDP sebaiknya bergerak dari sekadar kepatuhan terhadap regulasi menuju tata kelola pelindungan data yang benar-benar efektif: hak dapat digunakan, pengaduan dapat ditindaklanjuti, regulator mampu menegakkan aturan, organisasi dapat membuktikan kepatuhannya, dan masyarakat memiliki kemampuan praktis untuk melindungi serta menggunakan hak atas data pribadinya.

Roadmap Implementasi Lima Tahun (2027-2031)

Untuk menerjemahkan lima rekomendasi tersebut ke dalam tahapan yang realistis, Safe Nusa mengusulkan urutan implementasi lima tahun berikut. Tahapan ini bersifat berjenjang: fondasi kelembagaan dan koordinasi dibangun lebih dahulu, lalu diperkuat melalui penegakan, akses pemulihan, literasi yang terukur, serta tata kelola berbasis risiko yang adaptif terhadap perkembangan teknologi.

1 2027 berfokus pada fondasi kelembagaan dan koordinasi

Tindakan Prioritas: operasionalkan otoritas PDP; tetapkan pembagian peran dengan regulator sektoral dan aparat penegak hukum; siapkan SOP pengaduan, pemeriksaan, dan koordinasi; pastikan tersedia mekanisme transisi yang jelas untuk penerapan PP No. 33 Tahun 2026.

Indikator Kemajuan: otoritas beroperasi; mandat dan SOP koordinasi dipublikasikan; jalur pengaduan dan standar layanan tersedia.

2 2028 berfokus pada pengawasan berbasis risiko dan panduan sektoral

Tindakan Prioritas: terbitkan panduan implementatif untuk sektor dan pemrosesan berisiko tinggi; prioritaskan sektor yang memproses data sensitif atau berskala besar; perkuat fungsi DPO, asesmen dampak, pemetaan data, dan *privacy by design*.

Indikator Kemajuan: panduan sektoral tersedia; pengawasan berbasis risiko mulai diterapkan; organisasi prioritas memiliki mekanisme kepatuhan substantif.

3 2029 berfokus pada penegakan yang efektif dan mekanisme pemulihan yang mudah diakses

Tindakan Prioritas: perkuat kapasitas investigasi dan tindak lanjut pengaduan; publikasikan proses serta hasil penegakan secara transparan; ukur waktu penanganan kasus dan efektivitas pemulihan bagi subjek data.

Indikator Kemajuan: data pengaduan, waktu penyelesaian, tindakan korektif, dan hasil penegakan dipublikasikan secara berkala.

4 2030 berfokus pada literasi terukur dan adaptasi teknologi

Tindakan Prioritas: geser program literasi dari *awareness* menuju pengetahuan dan kemampuan praktis menggunakan hak; lakukan pengukuran berulang; keluarkan atau perbarui panduan untuk AI, *big data*, *blockchain*, transfer data lintas negara, dan teknologi intensif data lainnya.

Indikator Kemajuan: peningkatan pengetahuan objektif dapat diukur; panduan teknologi baru diperbarui berdasarkan risiko dan bukti implementasi.

5 2031 berfokus pada evaluasi efektivitas dan kematangan tata kelola

Tindakan Prioritas: lakukan evaluasi independen terhadap kapasitas otoritas, koordinasi antarlembaga, pola penegakan, kematangan kepatuhan organisasi, penggunaan hak oleh masyarakat, dan kebutuhan revisi kebijakan atau panduan.

Indikator Kemajuan: laporan evaluasi lima tahunan tersedia; rekomendasi perbaikan regulasi, kelembagaan, sumber daya, dan pengawasan ditindaklanjuti.

Roadmap ini tidak dimaksudkan sebagai lima agenda yang berdiri sendiri. Setiap tahap bergantung pada fondasi tahap sebelumnya, sementara evaluasi perlu dilakukan secara berulang agar pengawasan, kepatuhan, literasi, dan respons terhadap teknologi baru berkembang sebagai satu sistem tata kelola.

Referensi

Baquero, P. M., Wang, A., & Amariles, D. R. (2025). Unveiling transparency in data protection enforcement across the EU: Assessing the level and quality of disclosure of GDPR fines by data protection authorities. *European Law Journal, 31*(3), 177–202. https://doi.org/10.1111/eulj.70008

European Union Agency for Fundamental Rights. (2024). *GDPR in practice: Experiences of data protection authorities*. Publications Office of the European Union. https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities

Kementerian Komunikasi dan Digital. (2026, 22 Juli). *Wamen Nezar Patria: Indonesia siapkan otoritas pelindungan data pribadi yang independen*. https://portal.komdigi.go.id/kanal-publik/berita-kini/10412

Ma, S., & Chen, C. (2023). Are digital natives overconfident in their privacy literacy? Discrepancy between self-assessed and actual privacy literacy, and their impacts on privacy protection behavior. *Frontiers in Psychology, 14*, Artikel 1224168. https://doi.org/10.3389/fpsyg.2023.1224168

Peraturan Pemerintah Republik Indonesia Nomor 33 Tahun 2026 tentang Peraturan Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2026 Nomor 88 (2026).

Razi, F., Tuasikal, H., & Pratiwi Markus, D. (2024). Implementation and challenges of the Personal Data Protection Law in Indonesia. *Jurnal Indonesia Sosial Teknologi, 5*(12), 6559–6565. https://doi.org/10.59141/jist.v5i12.1285

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union, L 119*, 1–88 (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

Simbolon, V. A., & Juwono, V. (2022). Comparative review of personal data protection policy in Indonesia and the European Union General Data Protection Regulation. *Publik (Jurnal Ilmu Administrasi), 11*(2), 178–190. https://doi.org/10.31314/pjia.11.2.178-190.2022

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196 (2022). https://peraturan.bpk.go.id/Details/229798

Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law, 8*(2), 105–123. https://doi.org/10.1093/idpl/ipy002

Widiatedja, I. G. N. P., & Mishra, N. (2023). Establishing an independent data protection authority in Indonesia: A future-forward perspective. *International Review of Law, Computers & Technology, 37*(3), 252–273. https://doi.org/10.1080/13600869.2022.2155793