

Rekomendasi Kebijakan

Rancangan Undang-Undang Pelindungan Data Pribadi *Asosiasi E-Commerce Indonesia (IdEA)*

No.	Kategori	Pasal	Substansi	Analisis dan Usulan
1	Definisi Explicit Consent	- Pasal 20	<p>Isi pasal: Klausul perjanjian yang di dalamnya terdapat permintaan Data Pribadi yang tidak memuat persetujuan secara tegas (<i>explicit consent</i>) dari Pemilik Data Pribadi dinyatakan batal demi hukum.</p> <p>Catatan:</p> <ul style="list-style-type: none">• Persetujuan Data Pribadi juga terdapat dalam Pasal 17-21, Pasal 24 dan Pasal 49• Definisi dan cakupan Data Pribadi terdapat dalam Pasal 1 ayat 1 dan Pasal 3	<p>Mengacu kepada beberapa pengaturan terkait pelindungan data pribadi di dunia internasional, data pribadi yang bersifat “sensitif” membutuhkan <i>explicit consent</i>. Tujuannya adalah untuk memberikan pelindungan berlapis bagi data-data yang memiliki risiko signifikan atas hal dan kebebasan yang fundamental. Namun, dalam RUU PDP ini ketentuan mengenai <i>explicit consent</i> tidak terkait dengan kategorisasi tersebut.</p> <p>→ Ketentuan Data Pribadi Spesifik supaya disamakan konsepnya dengan GDPR. Dan <i>explicit consent</i> diarahkan hanya untuk pemrosesan Data Pribadi Spesifik.</p> <p>→ Definisi explicit consent dapat mengacu ke ketentuan “persetujuan yang sah” di dalam PP 71/2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yaitu: persetujuan yang disampaikan secara eksplisit, tidak boleh secara tersembunyi atau atas dasar kekhilafan, kelalaian, atau paksaan.</p>

2	Kewajiban Pengendali Data -Jangka Waktu Pemenuhan Hak	Pasal 24, 25, 26, 32, 34, 40	<p>Ketentuan-ketentuan ini mengatur tentang tata waktu untuk: (i) pemberitahuan oleh Pengendali Data pribadi terhadap perubahan informasi, (ii) penghentian pemrosesan data pribadi, (iii) penundaan dan pembatasan pemrosesan data pribadi, (iv) akses terhadap data pribadi yang diproses, perbaikan/pembaruan kesalahan dan/atau ketidakakuratan data pribadi, (v) pemberitahuan kegagalan perlindungan data pribadi.</p> <p>7 x 24 (tujuh kali dua puluh empat) jam untuk perubahan Informasi.</p> <p>3 x 24 (tiga kali dua puluh empat) jam untuk permintaan penarikan kembali persetujuan pemrosesan Data Pribadi.</p> <p>2 x 24 (dua kali dua puluh empat) jam untuk permintaan penundaan dan pembatasan pemrosesan Data Pribadi.</p> <p>3 x 24 (tiga kali dua puluh empat) jam untuk permintaan akses oleh Pemilik Data Pribadi.</p> <p>1 x 24 (satu kali dua puluh empat) jam untuk permintaan pembaruan dan/atau perbaikan Data Pribadi.</p>	→ Agar bisa mengakomodasi kepentingan semua skala bisnis, maka ketentuan jangka waktu seperti disebutkan di pasal-pasal tersebut agar dihapus, dan diatur lebih lanjut di peraturan teknis seperti Peraturan Pemerintah atau Peraturan Menteri/Badan.
---	--	------------------------------	--	---

			3 x 24 Menyampaikan pemberitahuan kegagalan perlindungan data	
3	Kewajiban Pengendali Data - Akurasi dan Verifikasi Data	Pasal 35	<p>a. Pengendali Data Pribadi wajib menjamin akurasi, kelengkapan, dan konsistensi Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan.</p> <p>b. Dalam menjamin akurasi, kelengkapan, dan konsistensi Data Pribadi sebagaimana dimaksud pada ayat (1) Pengendali Data Pribadi wajib melakukan verifikasi.</p>	<p>Verifikasi akurasi data seharusnya bukan menjadi kewajiban dari Pengendali Data Pribadi, melainkan pilihan yang bisa dilakukan oleh Pemilik Data Pribadi. Jika kewajiban akurasi data dibebankan pada Pengendali Data Pribadi, maka Pengendali akan mendapatkan lebih banyak data dari yang diharapkan dan tidak sesuai <i>data minimization</i> serta prinsip OECD. Hal juga akan menyulitkan UMKM, terutama yang tidak berbasis online.</p> <p>→ Pasal 35 dihapus.</p>
4	Kewajiban Pengendali Data - Pemulihan Data yang Dihapus	Pasal 38 Ayat 3	Data Pribadi yang telah dihapus sebagaimana dimaksud pada ayat (1) dapat dipulihkan atau ditampilkan kembali secara utuh dalam hal terdapat permintaan tertulis dari Pemilik Data Pribadi	<p>Secara praktik, data pribadi yang sudah dihapus tidak dapat dikembalikan/ dipulihkan lagi. Sehingga, ketentuan ini menjadi tidak implementatif.</p> <p>→ Pasal 38 ayat 3 dihapus</p>

5	Kewajiban Pengendali Data - Pengumuman Kegagalan Pelindungan Data	Pasal 40 Ayat 1	<p>Dalam hal terjadi kegagalan pelindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis dalam waktu paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada:</p> <p>a. Pemilik Data Pribadi; dan b. Menteri.</p>	<p>Pemberitahuan setiap kegagalan pelindungan Data Pribadi kepada kepada Menteri dan individu yang terkena dampak seharusnya didasarkan pada tingkat risiko yang ada. Dalam GDPR, pemberitahuan hanya diperlukan untuk pelanggaran keamanan yang memenuhi ambang batas bahaya minimum. Periode pemberitahuan adanya kegagalan pelindungan selama 3x24 jam terlalu kaku dan sulit diimplementasikan.</p> <ul style="list-style-type: none"> ● Best Practice Australia: pemberitahuan hanya diperlukan apabila ada kemungkinan "bahaya serius" bagi individu yang terdampak. ● Best Practice Kanada: pemberitahuan hanya diperlukan apabila ada "risiko nyata atas bahaya signifikan" bagi individu yang terdampak. ● GDPR Uni Eropa: memberikan beberapa fleksibilitas misalnya kerangka waktu 72 jam hanya berlaku "jika memungkinkan" dan hanya berlaku setelah entitas menyadari pelanggaran data. <p>→ Pemberitahuan pelanggaran kepada publik seharusnya tidak diperlukan jika notifikasi telah disampaikan kepada individu terkait dan/ atau pemerintah (kementerian).</p> <p>→ Pemberitahuan pelanggaran diberikan apabila menyangkut tingkat risiko yang tinggi (kebocoran data spesifik)</p>
---	--	--------------------	---	--

6	Sanksi	Pasal 61-69	Sanksi pidana dalam larangan penggunaan data pribadi	<p>→ Untuk mencegah adanya penyalahgunaan sanksi, maka perlu ada ketentuan terkait unsur kerugian terhadap pemilik data untuk hukuman pidana dan menjadikan sanksi pidana sebagai ultimum remedium.</p> <p>→ Pemerintah harus mengedepankan edukasi dalam mengurangi penyalahgunaan / pencurian data pribadi</p>
7	Komisi Independen dan Pembinaan	USULAN PASAL BARU	<p>Mendorong pembentukan komisi independen untuk menjalankan amanat undang-undang terkait perlindungan data pribadi.</p> <p>RUU ini belum secara jelas mengatur mengenai pembinaan yang akan dilakukan oleh pemerintah ataupun komisi independen apabila ada kebocoran data.</p> <p>Pembinaan merupakan suatu hal yang penting, untuk:</p> <ul style="list-style-type: none"> - mencegah kebocoran data di masa depan - sebagai catatan best practice bagi pemerintah untuk keamanan data. - mencegah terjadinya pidana yang tidak perlu. 	<p>→ Pembentukan komisi independen diharapkan mengakomodir unsur berbagai macam pemangku kepentingan dari pemerintah (Kemenkominfo dan BSSN) dan unsur non-pemerintah (pelaku bisnis, asosiasi, dan organisasi sipil) sebagai fungsi <i>check and balance</i> dan untuk menjaga independensi.</p> <p>→ Diusulkan untuk memasukan skema pembinaan dan insentif bagi pengelola data yang sudah melakukan pengelolaan data yang baik.</p>

8	Defini - Transfer Data ke Luar Negeri (TAMBAHAN)	Pasal 49	<p>a. Data Pribadi di luar wilayah hukum Negara Kesatuan Republik Indonesia dalam hal:</p> <ul style="list-style-type: none"> - negara tempat kedudukan Pengendali Data Pribadi atau organisasi internasional yang menerima transfer Data Pribadi memiliki tingkat perlindungan Data Pribadi yang setara atau lebih tinggi dari yang diatur dalam Undang-Undang ini; - terdapat perjanjian internasional antarnegara; - terdapat kontrak antar Pengendali Data Pribadi yang memiliki standar dan/atau jaminan perlindungan data pribadi sesuai dengan yang diatur dalam Undang-Undang ini; dan/atau - mendapat persetujuan Pemilik Data Pribadi. <p>b. Ketentuan lebih lanjut mengenai transfer Data Pribadi sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Pemerintah.</p>	<p>→ Diusulkan untuk dapat memasukan tambahan syarat diperbolehkannya transfer data pribadi ke luar negeri dengan <i>binding corporate rules</i> yang sudah berlaku di perusahaan di Indonesia yang tunduk dengan UU PDP dan ketentuan perundangan terkait informasi elektronik.</p>
---	---	----------	--	--

9	Definisi Keadaan Membahayakan (TAMBAHAN)	- Pasal 26 Ayat 2 (b)	<p>Penundaan dan pembatasan pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) dikecualikan dalam hal:</p> <ul style="list-style-type: none"> a. terdapat ketentuan peraturan perundang-undangan yang tidak memungkinkan dilakukan penundaan dan pembatasan pemrosesan Data Pribadi; b. dapat membahayakan keselamatan pihak lain; dan/atau <p>Pemilik Data Pribadi terikat perjanjian tertulis dengan Pengendali Data Pribadi yang tidak memungkinkan dilakukan penundaan dan pembatasan pemrosesan Data Pribadi</p>	<p>Ketentuan, “membahayakan keselamatan pihak lain”. Cakupan 'membahayakan keselamatan' bisa menimbulkan multi-interpretasi.</p> <p>→ Memperjelas ketentuan dalam Pasal 26 ayat 2 Huruf b terkait dengan frasa “membahayakan keselamatan pihak lain” yang dianggap sangat luas dari sisi cakupan dan subjek. Rekomendasi agar “Pihak Lain” diganti sebagai “subyek data”.</p>
---	---	-----------------------	---	---