Asosiasi FinTech Indonesia
(AFTECH)

Masukan dan Pandangan Industri Fintech atas Rancangan Undang-Undang Perlindungan Data Pribadi

Disusun untuk:
Rapat Dengar Pendapat Umum
Komisi I
Dewan Perwakilan Rakyat Republik Indonesia (DPR RI)
6 Juli 2020

I. Latar Belakang

Perlindungan data pribadi dan kerahasiaan data, telah menjadi perhatian penting seluruh penyelenggara fintech di Indonesia. Asosiasi Fintech Indonesia (AFTECH), melalui kelompok kerjanya, sejak tahun 2017 telah melaksanakan serangkaian dialog bersama dengan regulator dan stakeholder terkait, termasuk: Kementerian Komunikasi dan Informatika (Kemekominfo), Kementerian Koordinator Bidang Perekonomian (Kemenko Perekonomian), Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI).

Sejak awal Asosiasi Fintech Indonesia (AFTECH) bersama anggotanya sudah melakukan berbagai upaya dan inisiatif untuk menerapkan prinsip Perlindungan Data Pribadi. Dengan mengikuti berbagai Undang-undang, Peraturan Pemerintah maupun Peraturan Menteri terkait yang terkait dengan prinsip tata kelola data yang bertanggungjawab, termasuk di dalamnya keamanan siber dan perlindungan data pribadi konsumen seperti tercantum didalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika No. 20/2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, Peraturan Bank Indonesia 16/1/PBI/2014 tentang Perlindungan Konsumen Jasa Sistem Pembayaran, Peraturan OJK (POJK) 13/2018 Tentang Inovasi Keuangan Digital Di Sektor Jasa Keuangan, dan peraturan-peraturan lainnya. Selain itu, banyak dari penyelengara layanan fintech yang sudah melalui audit dan menerapkan standar international dalam upaya pengamanan data, seperti ISO 27001 yaitu standar sistem manajemen keamanan informasi.

Di dalam industri fintech, kenyamanan dan kepercayaan konsumen menjadi prioritas. Inovasi keuangan digital yang memberikan kenyamanan dan memberikan nilai tambah seyogyanya juga dapat dipertanggungjawabkan dengan baik. Industri Fintech sangat mendukung pembahasan dan pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi (PDP) dengan alasan – alasan sebagai berikut:

(a) Memberikan kepastian hukum terkait pengelolaan dan perlindungan data pribadi baik kepada konsumen fintech dan bagi penyelenggara fintech. Perlindungan data pribadi merupakan salah satu prinsip penting dalam tata kelola data yang sangat kritikal bagi perkembangan industri fintech serta inklusi keuangan nasional

(b) Prinsip tata kelola Perlindungan Data Pribadi dapat memberikan keseimbangan antara hak Pemilik Data Pribadi serta kepentingan Pengendali Data Pribadi. Pada akhirnya, diharapkan hal ini dapat meningkatkan kepercayaan masyarakat terhadap industri

(c) Undang-Undang Perlindungan Data Pribadi (PDP) dapat melindungi hak warga negara, serta dapat menjaga kedaulatan data nasional serta mendorong pertumbuhan ekonomi digital melalui peningkatan daya saing industri digital dalam negeri

(d) Rancangan Undang-Undang Perlindungan Data Pribadi (PDP) mendukung digitalisasi di Indonesia melalui kodifikasi ketentuan perlindungan Data Pribadi yang saat ini masih tersebar. Digitalisasi di segala lini akan semakin cepat terjadi, terutama sebagai akibat dari pandemi COVID-19 dan pemberlakuan New Normal. Oleh sebab itu dibutuhkan kerangka hukum yang dapat mendukung digitalisasi (terutama di sektor jasa keuangan) serta memastikan tanggungjawab penyelenggara sekaligus mengedepankan perlindungan konsumen

Dalam rangka mendukung terciptanya ekosistem ekonomi digital nasional yang baik serta inovasi keuangan digital yang bertanggung jawab melalui sistem tata kelola data baik, maka Asosiasi Fintech Indonesia (AFTECH) menyusun dan menyampaikan masukan dan pandangan industri fintech atas Rancangan Undang-Undang Perlindungan Data Pribadi (PDP).

II. Masukan dan Pandangan Umum Industri Fintech atas Rancangan Undang-Undang Perlindungan Data Pribadi

AFTECH menyambut baik cakupan dan isi dari Rancangan Undang-Undang Perlindungan Data Pribadi (PDP). AFTECH telah mengumpulkan masukan dari anggota AFTECH dan juga AFPI (Asosiasi Fintech Pendanaan Bersama Indonesia) yang menaungi Fintech Peer-to-Peer Lending. Secara garis besar terdapat 4 (empat) topik yang menjadi perhatian dari penyelenggara fintech di Indonesia:

a. <u>Sanksi Administratif dan Pidana</u>

AFTECH mendukung pemberian sanksi kepada para pelanggar, terutama dalam bentuk sanksi administratif, denda finansial dan penggantian ganti rugi kepada konsumen yang dirugikan. Pada saat yang sama AFTECH merekomendasikan agar sanksi dapat diterapkan secara proporsional dan tidak tumpang tindih dengan aturan perudangan lainnya. Salah satu usulan dari penyelenggara fintech

adalah untuk menghapus sanksi pidana badan yang ada dalam Pasal 61-69 RUU PDP

b. Kebutuhan akan penjabaran lebih lanjut beberapa pasal dalam RUU PDP

Guna meningkatkan pemahaman serta kepatuhan pelaku usaha terhadap RUU PDP dikedepannya, maka dibutuhkan penjelasan lebih detail dan/atau contoh-contoh atas beberapa pasal. Selanjutnya juga diperlukan informasi tambahan atas referensi peraturan perundang-undangan yang terkait dengan pelaksanaan RUU PDP. Diharapkan, dengan adanya penjelasan dan informasi tambahan ini akan mendorong implementasi RUU PDP yang lebih terukur, akuntabel dan bertanggung jawab.

Pasal-pasal yang membutuhkan penjelasan lebih lanjut diantaranya adalah tentang: subjek Undang-Undang; perbedaan pengaturan data pribadi secara umum dan spesifik; mekanisme pemrosesan, menghapus, dan/atau memusnahkan data pribadi; pemrosesan secara otomatis terkait profil seseorang (*profiling*); hak pemilik untuk menggunakan data pribadi (*introperabilitas*); pengajuan hak pemilik secara tertulis; persetujuan secara tegas (*explicit consent*); informasi yang wajib disampaikan untuk persetujuan; mekanisme menghentikan pemrosesan data pribadi atas permintaan pemilik; serta kewajiban menghapus data pribadi.

c. Terkait dengan implementasi, khususnya jangka waktu penghentian pemrosesan, pembatasan pemrosesan data pribadi, pemberian akses, serta pembaharuan data pribadi

Sebagai Undang-Undang nantinya Perlindungan Data Pribadi (PDP) ini nantinya akan berlaku di seluruh sektor usaha di Indonesia. Oleh sebab itu, penting untuk dipertimbangkan perbedaan kapabilitas dari masing-masing sektor usaha di Indonesia, serta perbedaan kapasitas dari tiap-tiap pelaku usaha yang ada. AFTECH berharap agar implementasi dari Undang-Undang Perlindungan Data Pribadi (PDP) ini dapat lebih mengakomodir keberagaman sektor dan pelaku usaha, serta berbagai kondisi dan situasi. Oleh sebab itu AFTECH menyampaikan rekomendasi agar hal ini dapat diatur lebih lanjut didalam peraturan pelaksanaan Undang-Undang.

d. Pengawasan terhadap Kepatuhan

Keberadaan komisi dan/atau badan independen yang mengawasi kepatuhan atau *compliant* secara menyeluruh adalah sangat penting guna menjamin efektivitas dan efisiensi dari implementasi Undang-Undang Perlindungan Data Pribadi (PDP).

III. Masukan Rinci atas Rancangan Undang-Undang Pelindungan Data Pribadi

Berikut ini adalah masukan rinci Asosiasi Fintech Indonesia (AFTECH) atas Rancangan Undang-Undang Pelindungan Data Pribadi:

NO.	RUU TENTANG PELINDUNGAN DATA PRIBADI	MASUKAN
1.	RANCANGAN UNDANG-UNDANG REPUBLIK INDONESIA NOMOR … TAHUN … TENTANG PELINDUNGAN DATA PRIBADI DENGAN RAHMAT TUHAN YANG MAHA ESA PRESIDEN REPUBLIK INDONESIA,	
2.	Menimbang: a. bahwa pelindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi, perlu diberikan landasan hukum yang kuat untuk memberikan keamanan atas data pribadi, berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;	
3.	b. bahwa pelindungan data pribadi ditujukan untuk menjamin hak warga negara atas pelindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi;	
4.	c. bahwa pengaturan data pribadi saat ini terdapat di dalam beberapa peraturan perundang-undangan maka untuk meningkatkan efektivitas dalam pelaksanaan pelindungan data pribadi diperlukan pengaturan mengenai pelindungan data pribadi dalam suatu undang-undang;	
5.	d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu membentuk Undang-Undang tentang Pelindungan Data Pribadi;	

6.	Mengingat: Pasal 5 ayat (1), Pasal 20, Pasal 28G ayat (1), Pasal 28H ayat (4), dan Pasal 28J Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;	
7.	Dengan Persetujuan Bersama DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA dan PRESIDEN REPUBLIK INDONESIA MEMUTUSKAN:	
8.	Menetapkan: UNDANG-UNDANG TENTANG PELINDUNGAN DATA PRIBADI.	
9.	BAB I KETENTUAN UMUM	
10.	Pasal 1 Dalam Undang-Undang ini yang dimaksud dengan:	Diusulkan adanya Pasal tambahan Pasal 1A (1) Undang-Undang ini berlaku untuk Pemrosesan Data Pribadi baik secara otomatis maupun non otomatis, termasuk pemrosesan Data Pribadi melalui mekanisme pseudonim. (2) Undang-undang ini tidak berlaku untuk: a. Pemrosesan Data Pribadi oleh orang perseorangan dalam rangka kegiatan keluarga; b. Pemrosesan data anonim; dan/atau c. Data agregat Pasal tambahan ini diperlukan untuk memberikan kejelasan ruang lingkup dari undang-undang ini. Pseudonim merupakan salah satu bentuk pelindungan data pribadi dengan cara menyamarkan subjek data. Subjek data yang sudah disamarkan dapat dikaitkan kembali dengan orang perorangan dengan menggunakan informasi tambahan yang digunakan untuk menyamarkan data tersebut. Oleh karena itu data pseudonim dianggap

		sebagai Data Pribadi karena dapat dikombinasikan dengan informasi tambahan untuk mengidentifikasi seseorang. Data anonim adalah data yang tidak berhubungan dengan seseorang atau data yang dibuat sedemikian rupa sehingga subjek data tidak atau tidak lagi dapat diidentifikasi. Data anonim bukan merupakan data pribadi karena bukan tentang seseorang dan tidak dapat digunakan untuk mengidentifikasi seseorang baik tersendiri atau dikombinasi dengan informasi lainnya secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik. Data agregat bukan merupakan data pribadi karena data agregat bukan merupakan data tentang seseorang. Merujuk pada GDPR Article 2 Ayat 2 Butir c, GDPR tidak berlaku untuk Data Pribadi yang digunakan dalam aktivitas personal atau household. Merujuk pada pertimbangan GDPR poin 26 disebutkan bahwa prinsip-prinsip perlindungan data tidak boleh diterapkan pada informasi anonim. Data agregat bukan merupakan data pribadi karena data agregat bukan merupakan data tentang seseorang dan tidak dapat digunakan untuk mengidentifikasi seseorang. Pemrosesan Data Pribadi menjadi data agregat perlu diatur sedemikian rupa sesuai aturan dalam RUU ini, tetapi apabila data sudah merupakan data agregat maka aturan dalam RUU ini tidak lagi berlaku
11.	1. Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik.	Definisi "Data Pribadi" seharusnya tidak mencakup data yang tidak dapat digunakan untuk mengidentifikasi orang tertentu/ perorangan yang dienkripsi, dianonimkan, tidak diidentifikasi, dan data pseudonym dengan beberapa alasan berikut:

		▪ Tidak selaras dengan *best practice* dalam mendukung pengembangan bisnis di era ekonomi digital modern dimana data sering digunakan untuk berinovasi karena penggunaan data tersebut berisiko rendah untuk pemilik data. ▪ Jenis data tersebut sangat penting bagi perusahaan dalam menganalisis data untuk meningkatkan produk, operasi, dan layanan bagi Konsumen. Memberlakukan perlindungan tambahan pada tipe data ini tidak secara signifikan menguntungkan privasi individu (karena tidak mengidentifikasi orang) tetapi dapat membatasi kemampuan bisnis untuk berinovasi dan bersaing secara efektif dalam ekonomi digital modern. Tidak disebutkan data pribadi item apa saja yang menjadi list data pribadi: e.g : nomor ktp, nama, alamat, nomor telefon, dll. Hanya merefer kepada UU ADMINDUK, sebagai suatu UU perlindungan data pribadi maka seharusnya dijelaskan objek yang disebut sebagai data pribadi secara komprehensif dan detil mengenai apa yang disebut data pribadi. Sehingga pelaku usaha dalam penyelenggaraannya secara jelas mengetahui Batasan-batasan untuk pengendalian dan pemrosesan data yang dikelola sehingga tidak ada multitafsir untuk definisi data pribadi. Kami merekomendasikan untuk mengubah definisi "Data Pribadi" untuk membatasinya dengan data yang berkaitan dengan orang alami yang diidentifikasi atau dapat diidentifikasi (dan tidak termasuk data yang terkait dengan perusahaan atau organisasi)

		Sehingga diusulkan menjadi, Data Pribadi adalah setiap data tentang orang **<u>perorangan</u>** baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung atau tidak langsung melalui sistem elektronik dan/atau non-elektronik, khususnya dengan merujuk pada pengidentifikasi seperti nama, nomor identifikasi, data lokasi, pengenal *online* atau satu atau lebih faktor spesifik terkait fisik, fisiologis, genetik, mental, ekonomi, budaya atau identitas sosial dari orang tersebut. Data Pribadi tidak termasuk data terenkripsi, anonim, tidak teridentifikasi, dan pseudonym.
12.	2. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.	Perbedaan antara "data" dan "informasi" perlu diperjelas. Terminologi yang digunakan harus disederhanakan menjadi "data" atau "informasi" Kami merekomendasikan perampingan terminologi yang digunakan di seluruh RUU baik untuk "data" atau informasi".
13.	3. Pengendali Data Pribadi adalah pihak yang menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.	
14.	4. Prosesor Data Pribadi adalah pihak yang melakukan pemrosesan Data Pribadi atas nama Pengendali Data Pribadi.	
15.	5. Pemilik Data Pribadi adalah orang perseorangan selaku subyek data yang memiliki Data Pribadi yang melekat pada dirinya.	Istilah kempemilikan data pribadi perlu diselaraskan dengan definisi lain yang digunakan dalam undang-undang privasi lainnya misalnya dalam EU GDPR Article 4 (1) - “orang perseorangan yang dapat diidentifikasi adalah orang yang dapat diidentifikasi secara langsung atau tidak langsung, khususnya dengan merujuk pada pengidentifikasi seperti nama, nomor identifikasi, data lokasi, pengenal

		online atau terhadap satu atau lebih faktor spesifik untuk identitas fisik, fisiologis, genetik, mental, ekonomi, budaya atau sosial dari perseorangan itu ” apabila data transaksi pengguna di marketplace selama 1 bulan dan jenis pembeliannya dapat diidentifikasi, itu masih dalam kepemilikan data pribadi orang perorangan atau sudah menjadi data milik penyelenggara marketplace? Diusulkan untuk tambahkan “.....yang memiliki data pribadi yang melekat pada dirinya **secara sah berdasarkan peraturan perundang-undangan yang berlaku”**
16.	6. Setiap Orang adalah orang perseorangan atau Korporasi.	
17.	7. Korporasi adalah kumpulan orang dan/atau kekayaan yang terorganisasi baik merupakan badan hukum maupun bukan badan hukum sesuai peraturan perundang-undangan.	apakah korporasi di sini mengacu kepada korporasi yang telah memiliki izin usaha melalui OSS? Diusulkan demikian, karena di beberapa peraturan perundang-undangan sudah mengatur hal demikian.
18.	8. Badan Publik adalah lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, atau organisasi nonpemerintah sepanjang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, sumbangan masyarakat dan/atau luar negeri.	
19.	9. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.	Perlu ditentukan badan independen penegak hukum perlindungan data pribadi untuk menciptakan kepastian hukum dalam implementasi peraturan ini nantinya. Kominfo yang merupakan bagian dari eksekutif, tidak memiliki

		fungsi penegakan hukum yang mana kewenangannya hanya akan terbatas dengan memberikan sanksi administratif, sehingga penegakan hukum peraturan ini akan sangat bergantung pada laporan masyarakat yang ini sangat bergantung pula pada kesadaran masyarakat mengenai pentingnya perlindungan data pribadi dan pengetahuan masyarakat terhadap pelanggaran dari pengendali data. Dengan adanya badan independent yang ditunjuk sebagai penegak hukum untuk peraturan ini, implementasi peraturan ini akan menjadi lebih efektif dan dapat tercapai pulalah tujuan diadakannnya peraturan ini. Diusulkan untuk ditambahkan definisi: - pelaku usaha (untuk define pengendali, pemroses, pemilik) atau subjek hukum yang dapat mengelola data atau menamfaatkan data. - pengatur sektor/instansi pengawas (untuk akomodir menteri selain kominfo yang meminta data kepada marketplace untuk masing-masing tujuan sektor tersebut.
20.	Pasal 2 Undang-Undang ini berlaku untuk Setiap Orang, Badan Publik, dan organisasi/institusi yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Negara Kesatuan Republik Indonesia maupun di luar wilayah hukum Negara Kesatuan Republik Indonesia, yang memiliki akibat hukum di wilayah hukum Negara Kesatuan Republik Indonesia dan/atau bagi Pemilik Data Pribadi Warga Negara Indonesia di luar wilayah hukum Negara Kesatuan Republik Indonesia.	Penjelasan mengenai subjek yang diatur di dalam RUU PDP ini apakah terbatas pada subjek di Indonesia dan/atau melakukan kegiatan di Indonesia atau subjek di luar Indonesia namun berdampak/berakibat hukum di Indonesia juga termasuk. Bagaimana penerapan untuk subjek di luar wilayah Indonesia yang mengakibatkan kerugian kepentingan Indonesia? Mohon agar dapat diklarifikasi mengenai subjek data pribadi yang dilindungi berdasarkan undang-undang ini – terutama terkait perbedaan dari kategori WNI yang disebutkan dalam a (ii) dan b

		(i) di bawah ini, apakah diperlukan adanya 'akibat hukum' terlebih dahulu sebelum peraturan ini berlaku terhadap WNI di luar negeri: a) Di wilayah Indonesia, berlaku terhadap: i. WNI dan WNA yang berada dalam wilayah hukum NKRI; dan ii. WNI dan WNA yang berada di luar wilayah hukum NKRI, dimana perbuatan hukum terkait pengaturan dalam UU perlindungan data pribadi memiliki akibat hukum di wilayah hukum NKRI. b) Di luar wilayah Indonesia: i. Pemilik data pribadi WNI di luar wilayah hukum NKRI Kami merekomendasikan amandemen Pasal 2 untuk mengklarifikasi bahwa undang-undang hanya berlaku jika: (1) penduduk Indonesia secara khusus ditargetkan; (2) data pribadi yang merupakan objek pemrosesan secara sengaja dikumpulkan dari data subyek di negara pada saat pengumpulan; dan (3) Pengumpulan tersebut dilakukan oleh entitas yang didirikan di negara tersebut melalui pengaturan yang stabil sehingga menimbulkan tingkat aktivitas yang nyata dan efektif.
21.	BAB II JENIS DATA PRIBADI	
22.	Pasal 3 (1) Data Pribadi terdiri atas:	Selain kewajiban ini, pengendali Data Pribadi dan prosesor data pribadi untuk menunjuk petugas perlindungan data pribadi, apakah

		terdapat perbedaan lainnya antara pengaturan data pribadi secara umum dan data pribadi secara spesifik? RUU PDP data pribadi mengacu pada UU ADMINDUK. Seharusnya dengan ditingkat UU, pendefinisian data pribadi tercantum secara jelas di dalam RUU PDP ini. E.g : pencantuman yang termasuk ke dalam data pribadi adalah nomor KTP, nomor telepon, nama lengkap, dll. Kemudian, pada Pasal (3) RUU PDP perlu dijelaskan lebih spesifik mengenai jenis-jenis data pribadi selain yang sudah dijelaskan dalam RUU PDP, yaitu terkait 3 jenis data pribadi antara lain: a. Data nasabah aktif b. Data nasabah tidak aktif c. Data nasabah mantan konsumen. Data-data ini dibutuhkan berkaitan dengan kepentingan regulasi para Penyelenggara LPMUBTI. Dan berdasarkan dengan ketentuan pidana yang telah diatur dalam RUU PDP ini, dapat ditambahkan definisi data pribadi secara spesifik, lengkap dan jelas untuk memberikan kepastian hukum. Contoh: 1) Nomor telepon seluler/alamat e-mail: Ketika nomor telepon seluler/alamat e-mail seseorang dipergunakan oleh orang lain untuk melakukan tindak pidana penipuan. Untuk penjabaran secara lengkap terkait definisi perlindungan data pribadi dapat diatur dalam Peraturan Pemerintah.
23.	a. Data Pribadi yang bersifat umum; dan	Definisi "Data Pribadi Umum" seharusnya dihapus karena RUU ini tidak membedakan antara perlakuan Data Pribadi Umum dan jenis-jenis Data Pribadi lainnya. Daftar lengkap dan tertutup yang mendefinisikan ruang lingkup "Data

		Pribadi Spesifik" direkomendasikan dan seharusnya tidak mencakup istilah umum seperti, "data lain sesuai dengan hukum dan peraturan". Diusulkan untuk dihapus atau diberikan penjelasan
24.	b. Data Pribadi yang bersifat spesifik.	
25.	(2) Data Pribadi yang bersifat umum sebagaimana dimaksud pada ayat (1) huruf a meliputi:	Perlu adanya definisi, kriteria dan perlakuan yang jelas terhadap klasifikasi data pribadi bersifat umum dan khusus. Data pribadi yang langsung berkaitan dengan identitas seseorang atau dapat mengidentifikasi seseorang serta digunakan secara umum oleh berbagai sektor diusulkan untuk dikategorikan sebagai data pribadi bersifat umum, sehingga data biometrik dan keuangan diusulkan untuk dikategorikan sebagai data pribadi bersifat umum.
26.	a. nama lengkap;	
27.	b. jenis kelamin;	
28.	c. kewarganegaraan;	
29.	d. agama; dan/atau	Diusulkan untuk dikategorikan sebagai data pribadi bersifat spesifik atau Jika berkaca kepada best practice yang ada, agama merupakan special categories of Personal Data
30.	e. Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang.	Usulan untuk poin ini dihapus. Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang memiliki ruang lingkup yang sangat luas. Disamping itu Bisa dimanipulasi untuk melakukan penerobosan privasi pribadi. Sehingga data Pribadi yang bersifat umum cukup poin a – d saja.
31.	(3) Data Pribadi yang bersifat spesifik sebagaimana dimaksud pada ayat (1) huruf b meliputi:	Perlu adanya definisi, kriteria dan perlakuan yang jelas terhadap klasifikasi data pribadi bersifat umum dan khusus. Data pribadi yang bersifat sensitif diusulkan untuk dikategorikan sebagai data pribadi bersifat umum, sehingga

		data agama diusulkan untuk dikategorikan sebagai data pribadi bersifat spesifik. Menyarankan untuk mengecualikan data keuangan yang jarang dipertimbangkan dalam kategori sensitif di yurisdiksi lain
32.	a. data dan informasi kesehatan;	
33.	b. data biometrik;	Diusulkan untuk dikategorikan sebagai data pribadi bersifat umum
34.	c. data genetika;	
35.	d. kehidupan/orientasi seksual;	Apa yang dimaksud dengan Data Pribadi kehidupan? Mengapa hal ini perlu diketahui?
36.	e. pandangan politik;	Untuk dihapus, karena sifatnya subyektif
37.	f. catatan kejahatan;	Setuju, untuk database kepolisian, kejaksaan, bea cukai dan pajak.
38.	g. data anak;	Kalau data anak ingin dilindungi, maka data istri/suami sebaiknya dilindungi juga karena kesulitan teknis untuk membuka data istri/suami tapi melindungi data anak
39.	h. data keuangan pribadi; dan/atau	Perlakuan data keuangan pribadi dalam kategori "data pribadi spesifik" dapat mengakibatkan bahaya yang tidak disengaja bagi pemilik data, sistem keuangan, dan pemerintah, dengan alasan sebagai berikut: • Pemrosesan data keuangan memiliki manfaat mendasar dan penting untuk pemilik data pribadi dan pelaku lain dalam ekonomi digital. Dengan menetapkan batasan yang ketat, akan menematkan industri keuangan Indonesia pada kerugian kompetitif yang signifikan dengan pesaing di negara lain yang tidak memiliki kendala serupa. • Data keuangan tidak dimasukkan sebagai data sensitif di berbagai hukum global, termasuk Undang-

		Undang Privasi Australia, Undang-Undang Jepang tentang Perlindungan Informasi Pribadi, Undang-Undang Perlindungan Informasi Pribadi Korea, Undang-Undang Perlindungan Data Pribadi Malaysia, dan UE GDPR. • Data keuangan dapat menginformasikan apakah pelanggaran data berisiko menimbulkan dampak material pada pemilik data. Berdasarkan pada berbagai kasus pelanggaran data A.S., pelanggaran yang melibatkan data keuangan (misal Informasi rekening bank, informasi kartu debit atau PIN) dapat dilaporkan, tetapi tidak tunduk pada persyaratan persetujuan lebih tinggi untuk data sensitif. • Tentang persyaratan persetujuan eksplisit: Pemilik data pribadi dapat menarik persetujuan mereka terhadap penggunaan data keuangan untuk tujuan pencegahan penipuan. Hal ini akan membuat mereka terbuka untuk situasi berbahaya dan akan mengurangi jumlah data yang tersedia untuk mengidentifikasi pola penipuan juga dapat menghambat upaya-upaya hukum oleh perusahaan untuk menyelidiki dan memulihkan utang. • Selain itu, data keuangan pribadi telah diatur ketat melalui sektor keuangan dan karenanya perlindungan tambahan melalui kerangka data pribadi - yang jauh lebih luas - semestinya tidak diperlukan. Dalam konteks GDPR, kategorisasi “data pribadi sensitif” dimaksudkan untuk memberikan proteksi tambahan atas data yang sifatnya “.... *could create*

		significant risks to the fundamental rights and freedom (of the data subjects)" - para 51. Apabila pengaturan data pribadi sensitif (atau dalam draft disebut "spesifik") di RUU PDP ini bermaksud sama, maka dalam kategorisasinya harus mengacu ke tujuan tersebut. Maka, "data keuangan pribadi" dan "data pribadi lainnya sesuai dengan ketentuan perundang-undangan" malah dapat membuat kategorisasi menjadi multi interpretasi dan tidak mengacu ke tujuan pengaturan yang ingin dicapai. Maka, sebaiknya dihapus atau diusulkan untuk dikategorikan sebagai data pribadi bersifat umum
40.	i. data lainnya sesuai dengan ketentuan peraturan perundangundangan.	Diperlukan penjelasan atau contoh "data lainya" serta referensi undang-undang terkait
41.	BAB III HAK PEMILIK DATA PRIBADI	
42.	Pasal 4 Pemilik Data Pribadi berhak meminta Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi.	Bagaimana guidelines dari pemerintah untuk tata cara permintaan informasi ini? misal berapa lama sejak permintaan informasi tersebut diajukan? apakah dengan syarat dan ketentuan yang tercantum sebelum pemilik data pribadi melakukan transaksi atau memberikan datanya kepada pelaku usaha tersebut sudah cukup? Apa Batasan atau definisi "kejelasan identitas" dan "akuntabilitas pihak yang meminta data pribadi"? Apakah pihak yang meminta Data Pribadi berbeda dengan Pengendali Data Pribadi?

43.	Pasal 5 Pemilik Data Pribadi berhak melengkapi Data Pribadi miliknya sebelum diproses oleh Pengendali Data Pribadi.	Apakah dalam hal ini pelaku usaha wajib menyediakan media dimana pemilik data pribadi dapat mengedit datanya sebelum submit dan diproses pelaku usaha laiknya seperti pengajuan kartu kredit di bank? Dan apakah hal ini berarti Pemilik Data Pribadi juga berhak untuk tidak melengkapi Data Pribadi miliknya sebelum pemrosesan?
44.	Pasal 6 Pemilik Data Pribadi berhak mengakses Data Pribadi miliknya sesuai dengan ketentuan peraturan perundang-undangan.	Bukankah ini menjadi kewajiban bagi Pengendali Data Pribadi untuk dapat memberikan akses kepada Pemilik Data Pribadi, sebagaimana dijelaskan pada Pasal 32. Apakah akan ada instrumen hukum lain yang membatasi hak akses Pemilik Data Pribadi? apa definisi mengakses? bagaimana tata cara agar pemilk data pribadi orang perorangan dapat mengakses datanya ke pelaku usaha? mohon dapat dijabarkan di penjelasan dan diberikan contoh agar pelaku usaha dapat mengerti konteks dari pengaksesan data tersebut. Contoh: apakah maksudnya pemilk data pribadi data mengecek riwayat transaksinya di marketplace? atau pemilk data pribadi dapat meminta akses data pribadinya ke sistem marketplace? untuk melindungi hak dari pelaku usaha sebaiknya diberikan Batasan untuk mengakses data pribadinya. Dalam hal memberikan hak akses dan Salinan tersebut, ada baiknya untuk diberikan jangka waktu kepada pelaku usaha dikarenakan apabila seluruh pemilik data pribadi diberikan hak akses dan Salinan data pribadi yang ada di pengendali maka akan memakan waktu yang tidak

		sebentar karena harus terlebih dahulu diproses.
45.	Pasal 7 Pemilik Data Pribadi berhak memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi miliknya sesuai dengan ketentuan perundang-undangan.	Bukankah ini menjadi kewajiban bagi Pengendali Data Pribadi untuk dapat memberikan akses kepada Pemilik Data Pribadi, sebagaimana dijelaskan pada Pasal 32. Apakah akan ada instrumen hukum lain yang membatasi hak akses Pemilik Data Pribadi Tambahan “wajib” karena data pribadi merefleksikan dan mengidentifikasi seseorang menghindari usangnya identitas seseorang. Kami mengusulkan pasal 7,8,9 dihapus secara keseluruhan dan diatur dalam Perilaku Privasi Industri atau peraturan Sektoral sebagaimana dimaksud dalam Pasal 55.
46.	Pasal 8 Pemilik Data Pribadi berhak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan Data Pribadi miliknya.	Apa ruang lingkup yang dimaksud pada pasal ini? Apakah ini berlaku hanya terhadap Data Pribadi yang dikelola oleh Pengendali, atau maksudnya disini lebih luas, yang artinya Pemilik Data Pribadi berhak untuk menghapus Data Pribadi-nya dalam hal apapun? Dalam hal ini pemusnahan data pribadi harus sesuai dengan mekanisme yang ada didalam Pengendali Data Pribadi. Tim teknis IT memerlukan waktu untuk develop hal ini dan peraturan ini perlu ada jangka waktu berlakunya agar pelaku usaha dapat develop hal ini di portal web masing-masing dan menanyakan kompleksitas developmentnya bagaimana. contoh: apabila si A tidak lagi menggunakan dan bertransaksi di marketplace A dan A meminta

		marketplace tersebut untuk menghapus akunnya dan segala data dan informasi si A. Perlu adanya pengaturan lebih lanjut mengenai hal ini, seperti pencantuman jangka waktu karena proses tersebut membutuhkan waktu dan yang lain. Sebagai contoh pada Penyelenggara LPMUBTI*:* apabila pada saat pemilik data pribadi telah mengajukan aplikasi dan memberikan data pribadi untuk diproses oleh Penyelenggara, dan data telah masuk dalam tahap pemrosesan oleh Penyelenggara, maka pemilik data pribadi tidak bisa secara langsung atau serta-merta melakukan penarikan data pada saat proses tersebut secara sepihak. Karena terdapat beberapa dampak terhadap Penyelenggara dalam memberikan Layanannya, seperti: 1. Penyelenggara lalai dalam pembuktian rekam jejak audit kepada regulator/pengawas, sebagaimana diatur dalam peraturan perundang-undangan terkait; dan 2. Menghambat efektivitas dan efisiensi biaya yang telah dikeluarkan Penyelenggara dalam hal pelaksanaan proses data pribadi tersebut.
47.	Pasal 9 Pemilik Data Pribadi berhak menarik kembali persetujuan pemrosesan Data Pribadi miliknya yang telah diberikan kepada Pengendali Data Pribadi.	Pada saat kapan dan/atau bagaimana pemilik data pribadi dapat menarik kembali persetujuan pemrosesan data pribadi miliknya? Hal ini dapat berpotensi mengganggu alur pemrosesan data yang ada di pelaku usaha. Data untuk profiling adalah data agregat sehingga akan menyita effort untuk menyaring pemilik data pribadi yang mengajukan keberatan tersebut.

		Dalam pasal 16 disebutkan hak pemilik data untuk menarik kembali persetujuan pemrosesan data dikecualikan jika untuk kepentingan proses penegakan hukum. Pada hakekatnya jika terjadi suatu kasus penegakan hukum kita tidak bisa membatasi data apa yang tidak bisa diberikan karena tergantung daripada kasus itu sendiri dan data yang dipunyai oleh pengendali data pribadi ybs Perlu ada ketentuan ketentuan bahwa Pemilik Data Pribadi memahami konsekuensi yang timbul dari Penarikan Kembali persetujuan pemrosesan data, serta dampak dan apabila ada proses hukum yang terkait. Disamping itu, perlu adanya aturan yang mengatur lebih jelas mengenai penghapusan data, dan penarikan kembali data pribadi oleh pemilik data. Sebagai contoh pada Penyelenggara LPMUBTI*:* apabila pada saat pemilik data pribadi telah mengajukan aplikasi dan memberikan data pribadi untuk diproses oleh Penyelenggara, dan data telah masuk dalam tahap pemrosesan oleh Penyelenggara, maka pemilik data pribadi tidak bisa secara langsung atau serta-merta melakukan penarikan data pada saat proses tersebut secara sepihak. Karena terdapat beberapa dampak terhadap Penyelenggara dalam memberikan Layanannya, seperti: 1. Penyelenggara lalai dalam pembuktian rekam jejak audit kepada regulator/pengawas, sebagaimana diatur dalam peraturan perundang-undangan terkait; dan 2. Menghambat efektivitas dan efisiensi biaya yang telah dikeluarkan Penyelenggara dalam hal pelaksanaan proses data pribadi tersebut.

48.	Pasal 10 Pemilik Data Pribadi berhak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis terkait profil seseorang (*profiling*).	Pemrosesan secara otomatis profil seseorang (profiling) ini seperti apa? apakah harus ada sistem untuk pemilik data dapat mengajukan keberatan atas tindakan pengambilan keputusan profiling Hal ini bertolak belakang dengan beberapa praktek di Industri yang membutuhkan profiling. 1. peraturan di P2P dimana sebagai perusahaan P2P diwajibkan untuk bekerja sama dengan credit scoring company untuk mendapatkan credit score yang mana credit score tersebut merupakan salah satu komponen profiling dalam rangka P2P memberikan layanan tambahan kepada customer. Dan untuk kepentingan penawaran produk dimana sebaiknya perusahaan menawarkan produk yang sesuai dengan kebutuhan dari customer itu sendiri. 2. Pemrosesan secara otomatis terkait profil nasabah dilakukan dari proses onboarding, transaksi sampai dengan pengajuan klaim dimana terdapat proses screening dan memonitor transaksi nasabah didasarkan pada profil nasabah tersebut melalui sistem. Profiling juga diperlukan untuk menentukan mapping antara kebutuhan nasabah dan profil nasabah yang sesuai dengan agen yang memasarkan dan produk yang ditawarkan. Apabila hak ini dibatasi maka perusahaan tidak bisa memberikan pelayanan yang terbaik kepada nasabah?

		Bahwa didalam RUU PDP Pasal 17 ayat 2 d disebutkan pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan; Sehingga keputusan yang diambil melalui pemrosesan secara otomatis merupakan keputusan yang akurat dan dapat dipertanggungjawabkan. Hak untuk mengajukan keberatan atas pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis dapat menghilangkan manfaat yang dapat diperoleh masyarakat, pemerintah dan industri serta dapat menghambat pertumbuhan ekonomi digital terutama bidang big data dan business intelligent, oleh karena itu perlu dibuat kaidah penggunaannya sehingga dapat terjadi keseimbangan antara hak Pemilik Data Pribadi dan kedudukan Pengendali Data Pribadi. Merujuk pada GDPR Artikel 22, hak Pemilik Data Pribadi untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis terkait profil seseorang (*profiling*) dibatasi penggunaanya. Hak tersebut dinyatakan tidak berlaku jika terdapat kontrak antara Pemilik Data Pribadi dengan Pengendali Data Pribadi, disahkan oleh *Union* atau *Member State*, terdapat persetujuan secara explisit dari Pemilik Data Pribadi Kami mengusulkan klausa ini dihapus secara keseluruhan, atau menambahkan pengecualian untuk mencakup persyaratan peraturan lainnya Atau Pada pasal 10 ditambahkan satu ayat sehingga berbunyi :

		Pasal 10 1. Pemilik Data Pribadi berhak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis terkait profil seseorang (*profiling*). 2. Hak Pemilik Data Pribadi sebagaimana dimaksud dalam Ayat 1 tidak berlaku jika: a. Diperlukan untuk pemenuhan kewajiban perjanjian dalam hal Pemilik Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Pemilik Data Pribadi pada saat akan melakukan perjanjian. b. Terdapat persetujuan secara explisit dari Pemilik Data Pribadi. Pemrosesan secara otomatis akan membawa manfaat yang besar bagi berbagai pihak baik pemerintah, masyarakat maupun industri diantaranya mempercepat layanan, menurunkan biaya, menghindari kesalahan manusia dan menghasilkan hasil yang lebih akurat, sehingga akan sangat bermanfaat untuk mengambil keputusan atau menentukan kebijakan.
49.	Pasal 11 Pemilik Data Pribadi berhak untuk memilih atau tidak memilih pemrosesan Data Pribadi melalui mekanisme *pseudonim* untuk tujuan tertentu.	Pseudonim merupakan salah satu bentuk pelindungan Data Pribadi dalam pemrosesan Data Pribadi. Apabila pemilik data diberikan hak untuk tidak memilih pemrosesan Data Pribadi melalui mekanisme pseudonim, maka hal ini justru akan memperlemah pelindungan Data Pribadi. Pseudonim harus di atus secara jelas, tegas dan terukur, karena hal ini bisa menjadi pintu manipulasi data. Kemudian RUU ini tidak mendefinisikan “data pseudonim”, tapi memasukan persyaratan tentang perlakuan terhadap data pseudonim pada Pasal

		11. Data anonim atau pseudonim tidak terindetifikasi dan tidak lagi terkait kepada individu tertentu (misalnya jika data sudah dikumpulkan, atau representasi dimasukkan ke dalam dataset). Mengeluarkan jenis data seperti itu akan memastikan bahwa organisasi memahami dengan benar apa yang merupakan data pribadi, sehingga mereka akan memfokuskan sumber daya mereka untuk melindungi dan menciptakan proses tata kelola yang sesuai untuk data pribadi. Lebih jauh, hak subyek data untuk menolak atau menyetujui 'nama samaran'akan menciptakan beban yang tidak semestinya bagi organisasi untuk membuat proses terpisah untuk penggunaan data non-pribadi. Persyaratan seperti ini akan menghalangi kegiatan bisnis organisasi yang valid dan tidak menambah perlindungan untuk Subyek Data. Kemudian, hak yang dimaksud dalam Pasal 11 tersebut juga diajukan melalui permintaan tertulis kepada Pengendali Data Pribadi atau dengan cara lain? 1. Merekomendasikan ketentuan ini dikecualikan untuk lembaga keuangan atau industri apa pun yang diawasi oleh Regulator Sektoral. 2. Pengecualian harus diperluas untuk memasukkan data anonim dan data pseudonim untuk peraturan ini Atau 3. Pasal ini tidak dimasukkan dalam UU PDP

50.	Pasal 12 Pemilik Data Pribadi berhak menunda atau membatasi pemrosesan Data Pribadi secara proporsional sesuai dengan tujuan pemrosesan Data Pribadi.	Pada saat kapan dan bagaiamana kondisi ini terjadi. Mohon penjelasan proporsi
51.	Pasal 13 Pemilik Data Pribadi berhak menuntut dan menerima ganti rugi atas pelanggaran Data Pribadi miliknya sesuai dengan ketentuan peraturan perundang-undangan.	Belum ada ketentuan perlindungan pelaku usaha apabila terjadi pelanggaran data pribadi melalui peretasan. Dalam hal ini apabila pelaku usaha menjadi korban peretasan atas data yang disimpannya. Hak pribadi yang berjalan bersamaan akan menyebabkan penegakan administrasi yang memberatkan di bawah Undang-Undang, tanpa batasan tentang jumlah atau freksuensi pengadu. Lebih lanjut, kemungkinan ada ketidakkonsistenan dalam menafsirkan Pasal ini akan memungkinkan para pelaku untuk memiliki wewenang yang luas, yang mengarah pada ketidakpastian antar bisnis di Indonesia. Disamping itu, dimohon kejelasan ketetapan untuk menghindari pertanggungjawaban ganda maupun terpisah, penghapusan pertanggungjawaban individu dan hukuman pidana, dan menggabungkan proses hukum serta mekanisme banding (Pasal 13, Pasal 51, dan Bab XIII). Oleh karena itu, kami merekomendasikan agar Pasal 13 dihapus secara keseluruhan. atau Kami merekomendasikan amandemen Pasal 16 untuk mengklarifikasi bahwa kuantum dan pemberian kompensasi tunduk pada proses pengadilan yang berlaku.
52.	Pasal 14 (1) Pemilik Data Pribadi berhak mendapatkan dan/atau menggunakan Data Pribadi miliknya dari Pengendali Data Pribadi dalam bentuk yang	Pemenuhan Pasal ini terlalu mahal apabila ingin dipenuhi. Artinya seluruh Pengendali Data Pribadi harus menyediakan format tertentu untuk Data

	sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik atau perangkat keras yang digunakan dalam interoperabilitas antar sistem elektronik.	Pribadi, dan harus memastikan bahwa seluruh Pengendali Data Pribadi lainnya dapat menerima format tersebut. Kami merekomendasikan untuk memasukkan dan menetapkan kriteria yang jelas Mendapatkan dan/atau menggunakan Data Pribadi miliknya dari Pengendali Data Pribadi – dapat diperjelas lagi secara maksud dan tujuannya contoh case di Singapore untuk email yang digunakan oleh pemilik data pribadi dapat dipindahkan dari email lama ke email baru (berbeda platform/penyelenggara). Hal ini dimungkinkan selama antar platform tersebut memungkinkan untuk diintegrasikan.
53.	(2) Pemilik Data Pribadi berhak menggunakan dan mengirimkan Data Pribadi miliknya ke Pengendali Data Pribadi lainnya, sepanjang sistem tersebut dapat saling berkomunikasi secara aman sesuai dengan prinsip pelindungan Data Pribadi berdasarkan Undang-Undang ini.	Kami merekomendasikan untuk menghapus atau menetapkan kriteria yang jelas. Terdapat beberapa pertanyaan: 1. Mohon klarifikasinya apakah yang dimaksud oleh Pasal 14(2) adalah Pemilik Data Pribadi berhak memberi perintah kepada suatu Pengandali Data Pribadi untuk mengirimkan Data Pribadi miliknya ke Pengendali Data Pribadi lainnya? 2. Apakah ini pemilik data pribadi dapat menggunakan informasi data pribadi miliknya digunakan di platform lainnya? 3. Bagaimana jaminan keamanannya jika platform memberikan akses untuk pemilik data pribadi menggunakan data pribadi milikinya untuk digunakan di platform lain? 4. Apakah platform harus memiliki mekanisme untuk sharing data pribadi? 5. Apakah harus ada perjanjian antara plaform untuk ketentuan ini?

54.	Pasal 15 Pelaksanaan hak Pemilik Data Pribadi sebagaimana dimaksud dalam Pasal 6 sampai dengan Pasal 10 dan Pasal 12 diajukan melalui permintaan tertulis kepada Pengendali Data Pribadi.	Hak ini melekat langsung pada pemilik data pribadi. Dalam hal pengajuan kepada pengendali data, maka pengendali data membutuhkan waktu untuk pemrosesan. Agar dapat dicantumkan jangka waktu tanggapan dari pengendali kepada pemilik data pribadi karena dalam pelaksanaannya pasti membutuhkan waktu dan perlu ditanyakan kepada tim teknis kesanggupannya di seluruh platform/portal web. Pasal 15 tidak memberikan informasi mengenai cara Pemilik Data Pribadi dapat melaksanakan haknya sebagaimana dimaksud dalam Pasal 11. Kami merekomendasikan revisi ketentuan untuk “permintaan tertulis yang diajukan ke pengawasan sektoral (OJK / Kementerian)” Atau Menambahkan kualifikasi pada efek bahwa di mana permintaan dari subjek data secara nyata tidak berdasar, terlalu membebani, atau berlebihan (mis., Karena permintaan berulang), pengontrol dapat Menagih biaya yang wajar dengan mempertimbangkan biaya administrasi penyediaan informasi atau komunikasi atau mengambil tindakan yang diminta; atau Menolak untuk bertindak atas permintaan. Pengontrol data akan menanggung beban untuk menunjukkan karakter permintaan yang tidak beralasan atau berlebihan.
55.	Pasal 16 (1) Hak-hak Pemilik Data Pribadi sebagaimana dimaksud dalam Pasal 8, Pasal 9, Pasal 10, Pasal 11, Pasal 12, dan Pasal 14 tidak berlaku untuk:	
56.	a. kepentingan pertahanan dan keamanan nasional;	Pengecualian terhadap kepentingan pertahanan dan keamanan nasional terlalu luas

57.	b. kepentingan proses penegakan hukum;	
58.	c. kepentingan umum dalam rangka penyelenggaraan negara;	Hal ini perlu dibatasi hanya untuk penyelenggaraan negara yang berdampak pada pemenuhan hak Pemilik Data Pribadi, sehingga pelaksanaan check and balances-nya untuk aspek ini dapat terpenuhi, karena apabila tidak ditentukan check and balances tidak terpenuhi dengan alasan: - Pemilik Data tidak dapat menolak karena tidak diminta persetujuan sementara validasi dari "tujuan penyelenggaraan negara" juga belum tentu berdampak pada hak Pemilik Data, sehingga apabila pemerintah menggunakan alasan ini sebagai validasi penggunaan data pribadi tanpa persetujuan, Pemilik menjadi tidak punya hak untuk mendapatkan remedi atas ketidaksetujuannya; - Tidak adanya badan independen penegak hukum peraturan ini, sehingga tidak ada yang dapat mengontrol pemerintah dalam pelaksanaannya, terlebih lagi Kominfo sebagai otoritas yang ditunjuk untuk menegakkan peraturan ini merupakan bagian dari eksekutif yang tidak memiliki fungsi penegakan hukum, sehingga check and balance khusus untuk hal ini tidak dapat terpenuhi.
59.	d. kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan; atau	Mengapa UU ini secara spesifik tidak mengatur industri jasa keuangan? Justru salah satu hal yang dibutuhkan masyarakat adalah pelindungan data pribadi untuk sektor jasa keuangan. Apakah akibat pengecualian pada huruf d artinya industri keuangan boleh mengabaikan ketentuan yang diatur pada pasal diatas? Hak privasi individu harus ditegakkan untuk sektor keuangan. Pengecualian

		hanya dalam kasus Pencucian Uang & Pendanaan Terorisme.
60.	e. agregat data yang pemrosesannya ditujukan guna kepentingan statistik dan penelitian ilmiah dalam rangka penyelenggaraan negara.	Pasal ini iusulkan untuk dihapus. Menurut hemat kami, hak-hak Pemilik Data Pribadi perlu untuk tetap terjamin dalam rangka untuk kepentingan statistik dan penelitian ilmiah mengingat informasi yang memuat data pribadi dalam hal ini tidak menjadi penentu dalam penyusunan data statistik dan penelitian ilmiah. Selain itu, hal ini tidak sesuai dengan *international best practice* Pasal 1 ayat 1 RUU PDP menyebutkan Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik. Berdasarkan definisi tersebut data agregat bukan merupakan data pribadi karena data agregat bukan merupakan data tentang seseorang, sehingga pengunaannya tidak perlu dibatasi. Pembatasan pemrosesan data agregat tidak membawa manfaat terhadap PDP tetapi justru dapat menghambat pertumbuhan industri digital Ketentuan pada huruf e redundan karena sudah dijelaskan pada huruf c dan tidak berlaku jika masih terdapat kewajiban yang timbul tanpa melawan hukum, yang dimana harus dipenuhi terlebih dahulu kepada Pengendali Data Pribadi Jika diwajibkan oleh undang - undang
61.	(2) Pengecualian sebagaimana dimaksud pada ayat (1) dilaksanakan hanya dalam rangka pelaksanaan ketentuan Undang-Undang.	

62.	BAB IV PEMROSESAN DATA PRIBADI	
63.	Pasal 17 (1) Pemrosesan Data Pribadi meliputi:	Beberapa istilah perlu diperjelaS termasuk perbedaan antara "perolehan dan pengumpulan" seperti yang digunakan dalam definisi "Pemrosesan Data Pribadi" dan apa yang disebut "jangka waktu retensi". Penjelasan untuk istilah ini agar disebutkan dalam penjelasan Pasal 17.
64.	a. perolehan dan pengumpulan;	
65.	b. pengolahan dan penganalisisan;	
66.	c. penyimpanan;	
67.	d. perbaikan dan pembaruan;	
68.	e. penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/atau	
69.	f. penghapusan atau pemusnahan.	
70.	(2) Pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) dilakukan sesuai dengan prinsip pelindungan Data Pribadi meliputi:	
71.	a. pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, patut, dan transparan.	Apa yang dimaksud transparan? Transparan bahwa dilakukan pengumpulan data apa, tapi tidak perlu disebutkan tekniknya bagaimana?
72.	b. pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya;	
73.	c. pemrosesan Data Pribadi dilakukan dengan menjamin hak Pemilik Data Pribadi;	
74.	d. pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan;	

75.	e. pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau kehilangan Data Pribadi;	
76.	f. pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan pelindungan Data Pribadi;	
77.	g. Data Pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan Pemilik Data Pribadi kecuali ditentukan lain oleh peraturan perundang-undangan; dan	Adanya kewajiban pemusnahan dan/atau penghapusan setelah berakhirnya masa retensi dengan periode tertentu sejalan dengan UU Dokumen Perusahaan dan UU Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang akan tetapi berdasarkan RUU PDP hal tersebut bisa didasarkan pada permintaan Pemilik Data Pribadi meskipun ditentukan oleh peraturan perundang-undangan akan tetapi kedudukan keduanya sebagai UU menjadi kendala menentukan acuan yang mana. Dalam hal suatu data pribadi dihapuskan maka pemilik data pribadi tidak dapat lagi mendapatkan pelayanan dari perusahaan dan pertanggungan yang dikelola yang diberikan oleh perusahaan harus berakhir. Harap ditambahkan ketentuan bahwa pemilik data pribadi mengerti konsekuensi yang timbul akibat permintaan tersebut. Perlu diinformasikan referensi peraturan perundang-undangan yang menjelaskan mengenai ketentuan masa retensi data pribadi. Seperti batas waktu retensi dimasukkan agar lebih jelas
78.	h. pemrosesan Data Pribadi dilakukan secara bertanggung jawab dengan memenuhi pelaksanaan prinsip pelindungan Data Pribadi dan dapat dibuktikan secara jelas.	

79.	(3)Ketentuan teknis pelaksanaan pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) diatur oleh Menteri.	Rancangan Peraturan Menteri perlu disusun secara parallel dengan RUU sehingga tidak tertinggal ketika di lakukan implementasi UU ini.
80.	Pasal 18 (1) Pemrosesan Data Pribadi sebagaimana dimaksud dalam Pasal 17 harus memenuhi ketentuan adanya persetujuan yang sah dari Pemilik Data Pribadi untuk satu atau beberapa tujuan tertentu yang telah disampaikan kepada Pemilik Data Pribadi.	Bentuk persetujuannya apakah dapat berbentuk elektronik atau wajib tertulis basah? Kerangka persetujuan seharusnya dibuat lebih sederhana dan seharusnya mengakui persetujuan tersirat/ *implied consent*. Pasal belum mencakup dasar kepentingan yang sah (misal dimana pemrosesan diperlukan untuk kepentingan sah pengendali). Seharusnya persetujuan mengakui dan memungkinkan pemrosesan data untuk kepentingan bisnis yang sah, seperti, kewajiban hukum, manajemen risiko dan tujuan lain yang selaras dengan harapan pemilik data pribadi dan/atau keadaan transaksi. Jenis persetujuan atau consent berbeda untuk setiap kasus. Untuk itu, beberapa contoh persetujuan atau consent yang valid harus diberikan dalam Penjelasan atau Peraturan Menteri.
81.	(2) Persetujuan sebagaimana dimaksud pada ayat (1) tidak diperlukan dalam hal pemrosesan Data Pribadi untuk:	Persetujuan hanya diperlukan untuk kasus penggunaan spesifik tertentu untuk memastikan bahwa pemrosesan data dasar untuk layanan agar berfungsi tetap tersedia. Misalnya, beberapa pemrosesan data diperlukan untuk membuat produk berfungsi dan memastikan bahwa mereka aman dan dapat diandalkan Penelitian tentang "*consent fatigue*" menunjukkan bahwa semakin banyak permintaan untuk persetujuan, semakin sedikit perhatian individu atas permintaan untuk meberikan persetujuan. Pengguna umumnya dapat menerima dan bahkan mengharapkan

		dan menganggapnya wajar bahwa beberapa informasi pribadi perlu diproses oleh perusahaan yang menyediakan produk atau Layanan. Pengecualian juga harus mencakup keadaan berikut: (i) Situasi yang mengancam jiwa; (ii) AML / CTF, Pencegahan Penipuan atau persyaratan peraturan lainnya; atau (iii) Domain Publik
82.	a. pemenuhan kewajiban perjanjian dalam hal Pemilik Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Pemilik Data Pribadi pada saat akan melakukan perjanjian;	
83.	b. pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;	
84.	c. pemenuhan pelindungan kepentingan yang sah (vital interest) Pemilik Data Pribadi;	
85.	d. pelaksanaan kewenangan Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;	
86.	e. pemenuhan kewajiban Pengendali Data Pribadi dalam pelayanan publik untuk kepentingan umum; dan/atau	
87.	f. pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan Pengendali Data Pribadi dan hak Pemilik Data Pribadi.	Perlu diperjelas: 1. Siapa yang menentukan apakah suatu kepentingan pemrosesan data adalah sah? 2. pemenuhan kepentingan yang sah lainnya = kalimat ambigu. Harus mengacu pada pasal 16 RUU PDP ini Menambahkan dasar yang sesuai dengan ketentuan “kepentingan sah” dalam EUGDPR Pasal 6. Dalam banyak kasus, kepentingan yang sah dapat memberikan standar perlindungan privasi lebih karena perlunya pengendali data untuk menyeimbangkan hak dan kebebasan individu terhadap

		kepentingan organisasi yang memproses data dan membenarkan pemrosesan berdasarkan persetujuan tersebut.
88. .	Pasal 19 (1) Persetujuan pemrosesan Data Pribadi dilakukan melalui persetujuan tertulis atau lisan terekam.	Persetujuan tertulis, secara elektonik yang tervalidasi misalnya dengan memasukkan nomor induk kependudukan. Dasar hukum tambahan ini juga diperlukan untuk memastikan bahwa perkembangan teknologi, khusutnya IoT, didukung oleh pengumpulan informasi pribadi yang legal. Kami juga menggarisbawahi bahwa dasar hukum tersebut merupakan pengecualian untuk persyaratan persetujuan. Semua dasar hukum yang ditetapkan dalam undang-undang untuk mengumpulkan, menggunakan dan mengungkapkan data pribadi harus diperlakukan sama, dan tidak mengandalkan persetujuan sebagai landasan utama untuk memproses data pribadi. Persyaratan yang terlalu ketat untuk persetujuan akan memperlambat penyediaan barang dan jasa kepada customer dan meningkatkan biaya pemenuhan tanpa meningkatkan keamanan untuk subyek data. Oleh karena itu kami merekomendasikan bahwa RUU ini diperluas hingga mencakup (tapi tidak terbatas pada) dasar-dasar untuk pemrosesan berikut ini: (i) pencegahan dan deteksi segala aktivitas yang melanggar hukum termasuk penipuan; (ii) pengumpulan jika diperlukan untuk tujuan evaluatif; dan (iii) pemrosesan jika diperlukan untuk keperluan kepentingan yang valid yang dilakukan oleh Personal Data Controller, Personal Data Processor, atau pihak ketiga. Selain itu, Pasal 19 dan 20 juga harus diubah untuk memungkinkan

		persetujuan yang diberikan maupun yang tersirat. Persetujuan ‘tertulis’ atau ‘terekam secara verbal’ mungkin tidak selalu dapat dipraktikkan dan persyaratan seperti itu akan secara signifikan memengaruhi kemudahan berbisnis. Misalnya, ketika Subyek Data menyerahkan kartu kredit kepada retailer untuk memproses pembayaran, persetujuan mereka untuk pengumpulan, penggunaan dan pengungkapan data pribadi mereka (yaitu data pembayaran kartu kredit) untuk keperluan pemrosesan pembayaran dapat diimplikasikan melalui tindakan mereka. Akan sangat memberatkan bagi retailer jika mereka diwajibkan untuk memberi tahu, menjelaskan, dan merekam persetujuan eksplisit untuk setiap proses pembayaran. Persyaratan seperti itu akan secara signifkan menghambat kemudahan berbisnis, dan tidak memberikan perlindungan tambahan untuk subyek data. The Singapore Personal Data Protection Act (2012), memasukkan dasar persetujuan yang diberikan di bawah Section 15, di mana persetujuan subyek data bisa "dipertimbangkan" jika subyek data secara sukarela menyediakan data untuk suatu tujuan dan masuk akal dilakukan oleh subyek data. Oleh karena itu kamu merekomendasikan agar Pasal 19 dan 20 diubah dengan memasukkan konsep persetujuan yang diberikan dan yang tersirat. Melakukan hal ini akan memastikan bahwa hak Subyek Data tetap terlindungi, tanpa secara signifikan menghambat kemudahan atau kecepatan berbisnis.
89.	(2) Persetujuan tertulis sebagaimana dimaksud pada ayat (1) dapat disampaikan secara elektronik atau nonelektronik.	Perlu diperjelas mengenai standar minimum mekanisme penyampaian persetujuan tertulis secara elektronik guna memberikan kejelasan terkait

		teknis pelaksanaan pemberian persetujuan tertulis tersebut.
90.	(3) Persetujuan tertulis dan lisan terekam sebagaimana dimaksud pada ayat (1) mempunyai kekuatan hukum yang sama.	
91.	(4) Dalam hal persetujuan tertulis sebagaimana dimaksud pada ayat (1) di dalamnya memuat tujuan lain, permintaan persetujuan harus memenuhi ketentuan:	Mengusulkan Pengendali Data untuk menyediakan format dan sarananya. Menurut hemat kami, konteks “tujuan lain" perlu dijelaskan lebih detil atau perlu diberikan contoh yang dimaksud dengan “tujuan lain"
92.	a. dapat dibedakan secara jelas dengan hal lainnya;	Perlu diuraikan lebih lanjut mengenai *explicit consent* karena penjelasan ini tidak ditemukan baik di draf UU dan penjelasan, serta naskah akademik UU.
93.	b. dibuat dengan format yang dapat dipahami dan mudah diakses; dan	
94.	c. menggunakan bahasa yang sederhana dan jelas.	
95.	(5) Persetujuan yang tidak memenuhi ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (4) dinyatakan batal demi hukum.	Di sini juga harus ada satu pasal yang menyebutkan bahwa Pihak Ketiga dapat mengakses Data Pribadi hanya dengan persetujuan dari pemilik Data Pribadi. Ini juga bisa berupa persetujuan tambahan di luar persetujuan atau consent valid yang diambil dari Pemilik Personal Data. Ini akan membantu memberikan layanan yang telah disesuaikan untuk customer.
96.	Pasal 20 Klausul perjanjian yang di dalamnya terdapat permintaan Data Pribadi yang tidak memuat persetujuan secara tegas (*explicit consent*) dari Pemilik Data Pribadi dinyatakan batal demi hukum.	Persetujuan oleh pemilik data pribadi adalah hal terpenting dalam pemrosesan data pribadi. Sesuai dengan ketentuan yang terdapat dalam berbagai regulasi terkait data pribadi di berbagai negara, persetujuan disebutkan tidak selalu harus berbentuk eksplisit. Persetujuan eksplisit (explicit consent), di mana pemilik data pribadi harus menyatakan persetujuannya secara ekspresif, hanya dipersyaratkan untuk

		pemrosesan data pribadi yang sifatnya sensitif. Dalam RUU PDP ini terdapat dua isu terkait dengan hal ini: i) cakupan data pribadi spesifik yang tidak jelas; serta ii) konsep explicit consent yang tidak jelas Explicit Consent : Mengacu kepada beberapa pengaturan terkait perlindungan data pribadi di dunia internasional, data pribadi yang bersifat "sensitif" membutuhkan explicit consent . Tujuannya adalah untuk memberikan perlindungan berlapis bagi data-data yang memiliki risiko signifikan atas hal dan kebebasan yang fundamental. Namun, dalam RUU PDP ini ketentuan mengenai explicit consent tidak terkait dengan kategorisasi tersebut. Implementasi ketentuan pasal ini sulit untuk dilakukan mengingat "persetujuan secara tegas (*explicit consent*)" tersebut dapat diartikan dengan berbagai interpretasi maupun dicantumkan dalam syarat dan ketentuan (*terms & conditions*) yang pada pelaksanaannya diberikan dalam bentuk klausul general.Terkait hal ini, diperlukan kejelasan atas informasi atau ketentuan minimum yang wajib ada di dalam klausul perjanjian. Apakah akan mengacu kepada Pasal 1331 dan Pasal 1320 KUHPerdata. 1. Ketentuan tentang "tidak memuat persetujuan" bertolak belakang dengan pasal 18 ayat (2). 2. Apakah yang dimaksud secara tegas (*explicit consent*)? Berkaca kepada *best practice* internasional, ketentuan *explicit consent* digunakan untuk kasus tertentu, dan memiliki persyaratan khusus dibandingkan persetujuan pada umumnya. Apabila seluruh persetujuan untuk memproses data memerlukan *explicit*

		consent, maka dampak yang akan terjadi adalah sebagai berikut: Seluruh proses persetujuan yang sebelumnya dapat menggunakan *implied consent* sekarang wajib menggunakan *explicit consent*. Sebagai contoh, dalam hal Anda meminta kartu nama, maka Anda harus meminta *explicit consent* untuk meminta data tersebut, dimana hal tersebut dapat dipenuhi dengan *implied consent*, dimana apabila suatu individu memberikan kartu namanya, maka dia secara implisit telah memberikan persetujuan (*implied consent*) agar data yang terdapat dalam kartu namanya dapat digunakan. Masukan: • Ketentuan Data Pribadi Spesifik supaya disamakan konsepnya dengan GDPR. Dan explicit consent diarahkan hanya untuk pemrosesan Data Pribadi Spesifik. • 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
97.	Pasal 21 (1) Dalam melakukan pemrosesan Data Pribadi, Pengendali Data Pribadi wajib menjaga kerahasiaan Data Pribadi.	Berdasarkan ayat (2) huruf a, apakah artinya tidak ada kerahasiaan data untuk bidang ketenagakerjaan, jaminan sosial, perpajakan, pengawasan sektor termasuk sektor keuangan, penyelenggaraan administrasi kependudukan, dan/atau kesejahteraan social?
98.	(2) Ketentuan mengenai kewajiban menjaga kerahasiaan Data Pribadi sebagaimana dimaksud pada ayat (1) dikecualikan dalam hal:	

99.	a. Pemilik Data Pribadi telah memberikan persetujuan sebagaimana dimaksud dalam Pasal 19;	Jadi kalau setuju melakukan pemrosesan data pribadi (pasal 19), maka tidak perlu menjaga kerahasiaan data pribadi? Kelihatannya definisi “merahasiakan/ kerahasiaan” harus didefinisikan: merahasiakan dari siapa atau apa, apanya yg dirahasiakan (Data pribadinya?)
100.	b. diperlukan untuk tujuan melaksanakan kewajiban dan/atau hak tertentu dari Pengendali Data Pribadi atau dari Pemilik Data Pribadi di bidang ketenagakerjaan, jaminan sosial, perpajakan, pengawasan sektor termasuk sektor keuangan, penyelenggaraan administrasi kependudukan, dan/atau kesejahteraan sosial yang memberikan pelindungan terhadap hak dasar dan kepentingan Pemilik Data Pribadi;	
101.	c. diperlukan untuk melindungi kepentingan Pemilik Data Pribadi yang tidak cakap baik secara fisik maupun hukum; dan/atau	
102.	d. diperlukan untuk kepentingan proses penegakan hukum.	
103.	(3) Pengecualian sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.	Menurut hemat kami, perlu diinformasikan referensi peraturan perundang-undangan yang menjelaskan mengenai ketentuan pelaksanaan “pengecualian" sebagaimana dijelaskan pada ayat (2)
104.	Pasal 22 (1) Pemasangan alat pemroses atau pengolah data visual di tempat umum dan/atau pada fasilitas pelayanan publik dilakukan dengan ketentuan:	1. Apakah hanya terhadap pemrosesan atau pengolahan data visual? 2. Apakah batasan “tempat umum”? 3. Apakah definisi “fasilitas pelayanan publik”? 4. bagaimana pemenuhan persetujuan dalam hal pemasangan alat pemroses data visual tersebut? 5. Bagaimana dengan pemasangan kamera cctv didalam kantor atau diluar rumah?
105.	a. untuk tujuan keamanan, pencegahan bencana, dan/atau penyelenggaraan lalu	

	lintas atau pengumpulan, analisis dan pengaturan Informasi lalu lintas;	
106.	b. harus menampilkan Informasi bahwa pada area tersebut telah dipasang alat pemroses atau pengolah data visual; dan	
107.	c. tidak digunakan untuk mengidentifikasi seseorang.	Menyarankan untuk menambahkan c. tidak digunakan untuk mengidentifikasi seseorang, kecuali untuk alasan sebagaimana dimaksud pada ayat (1) huruf a Pasal 22 ini.
108.	(2) Ketentuan sebagaimana dimaksud pada ayat (1) huruf b dan huruf c dikecualikan untuk pencegahan tindak pidana dan proses penegakan hukum sesuai dengan ketentuan peraturan perundang-undangan.	
109.	BAB V KEWAJIBAN PENGENDALI DATA PRIBADI DAN PROSESOR DATA PRIBADI DALAM PEMROSESAN DATA PRIBADI	
110.	Bagian Kesatu Umum	
111.	Pasal 23 Pengendali Data Pribadi dan Prosesor Data Pribadi meliputi:	Organisasi Internasional dalam konteks ini juga harus relevan untuk Personal Data Controller dan bukan Personal Data Processor.
112.	a. Setiap Orang;	Individu rentan penyalahgunaan.
113.	b. Badan Publik; dan	
114.	c. organisasi/institusi.	Perlu diberikan penjelasan lebih lanjut mengenai cakupan organisasi/institusi, apakah dalam hal ini pelaku usaha/korporasi termasuk di dalam cakupan poin ini.
115.	Bagian Kedua Kewajiban Pengendali Data Pribadi	
116.	Pasal 24 (1) Dalam rangka mendapatkan persetujuan sebagaimana dimaksud dalam Pasal 18 ayat (1),	Apa maksud legalitas pemrosesan Data? Apa yang membedakannya dengan tujuan pemrosesan Data?

	Pengendali Data Pribadi wajib menyampaikan Informasi mengenai:	Berdasarkan UU Administrasi Kependudukan yang mengatur hak akses lembaga swasta terhadap NIK, Data Kependudukan dan KTP elektronik seluruh WNI, melalui mekanisme MOU kerjasama lembaga, akan bertentangan dengan RUU PDP dikarenakan tidak diakomodirnya persetujuan dari pemilik data. Pasal 24 juga mengharuskan Personal Data Controller untuk memberikan daftar informasi tertentu kepada subyek data sebelum mendapatkan persetujuan. Persyaratan ini harus menghindari formulasi berlebihan, dan harus juga mengatasi keadaan di mana persetujuan dapat dianggap sah (sebagaimana ditunjukkan dalam contoh sebelumnya pada pemrosesan pembayaran), atau di mana sebuah organisasi melakukan pemrosesan dengan mengandalkan dasar-dasar lain selain persetujuan.
117.	a. legalitas dari pemrosesan Data Pribadi;	Perlu untuk diberikan penjelasan lebih lanjut mengenai “informasi legalitas dari pemrosesan Data Pribadi”.
118.	b. tujuan pemrosesan Data Pribadi;	
119.	c. jenis dan relevansi Data Pribadi yang akan diproses;	
120.	d. periode retensi dokumen yang memuat Data Pribadi;	Batas waktu retensi dimasukkan agar lebih jelas
121.	e. rincian mengenai Informasi yang dikumpulkan;	Diusulkan untuk Dihapus Persetujuan yang terlalu banyak, rinci dan komplek akan membuat seseorang tidak peduli dengan isinya, sehingga cenderung setuju tanpa memahami isi persetujuan, hal ini justru dapat merugikan Pemilik Data Pribadi. Rincian mengenai informasi yang dikumpulkan sudah dapat diwakili dengan jenis dan relevansi Data Pribadi

		yang akan diproses serta tujuan pemrosesan Data Pribadi.
122.	f. jangka waktu pemrosesan Data Pribadi; dan	Diusulkan untuk Dihapus Jangka waktu pemrosesan data pribadi akan sangat dinamis, jika terjadi beberapa kali perubahan jangka waktu pemrosesan dan harus diinformasikan kepada Pemilik Data Pribadi, maka hal ini malah dapat mengganggu kenyamanan Pemilik Data Pribadi. Secara keseluruhan jangka waktu pemrosesan Data Pribadi sudah dapat diwakili dengan periode retensi dokumen yang memuat Data Pribadi
123.	g. hak Pemilik Data Pribadi.	Perlu diberikan penjelasan lebih lanjut mengenai hak Pemilik Data Pribadi. Apakah hanya mencakup hak-hak Pemilik Data Pribadi sebagaimana tercantum dalam RUU PDP ini. Penyampaian informasi hak Pemilik Data Pribadi cukup dilakukan dengan menyebutkan nomor dan tahun undang-undang yang digunakan sebagai rujukan.
124.	(2) Dalam melakukan pemrosesan Data Pribadi, Pengendali Data Pribadi wajib menunjukkan bukti persetujuan yang telah diberikan oleh Pemilik Data Pribadi.	Definisi menunjukkan bukti persetujuan seperti apa dan spesifikasinya dalam bentuk apa? mohon dapat dicantumkan di sini atau di bagian penjelasan. Kepada siapa bukti persetujuan tersebut ditunjukkan? Perlu diberikan contoh bukti persetujuan (yang sah secara hukum / yang diperbolehkan) yang telah diberikan oleh pemilik data pribadi khususnya apabila persetujuan diberikan secara elektronik Menyarankan untuk mengklarifikasi bagaimana persetujuan yang disyaratkan dalam Pasal 24 dapat 'ditampilkan' dan juga pengecualian apa yang berlaku untuk persyaratan untuk menampilkan persetujuan.

		Atau dihapus karena persyaratan untuk mendapatkan "bukti persetujuan" sebelum pengumpulan data itu berat dan tidak praktis jika data controller mengandalkan persetujuan atau dasar-dasar lainnya.
125.	(3) Dalam hal terdapat perubahan Informasi sebagaimana dimaksud pada ayat (1), Pengendali Data Pribadi wajib memberitahukan kepada Pemilik Data Pribadi paling lambat 7 x 24 (tujuh kali dua puluh empat) jam setelah terjadi perubahan Informasi.	Jangka waktu ini terlalu restriktif kami mengusulkan agar dapat diubah menjadi paling lambat 1 bulan sesuai dengan *international best practice* (termasuk GDPR). Selain itu, menurut hemat kami tidak semua Pengendali Data Pribadi mempunyai sistem dan/atau SDM yang mencukupi untuk melakukan hal tersebut. Pada prakteknya misal, organisasi mungkin memiliki timeline sendiri dalam memverifikasi identitas pemohon, siklus akuntansi, dan penutupan akun (misalnya 14 atau 21 hari), dan mengkonsolidasikan semua informasi yang diminta juga akan memakan waktu (misalnya, jika pemohon meminta sejumlah besar informasi yang terkandung dalam berbagai sumber). Oleh karena itu kami merekomendasikan agar RUU tidak menjadi terlalu preskriptif dan menghapus penetapan kerangka waktu yang terlalu spesifik. GDPR memberikan waktu **satu bulan sejak permohonan diterima,** dan **dapat diperpanjang dua bulan.** Sedangkan, PDPA Malaysia memberikan waktu 21 hari (dan dapat diperpanjang). **Masukan:** Disamakan dengan GDPR/ PDPA Malaysia Dan

		Perubahan yang terjadi karena dilakukan oleh pemilik data pribadi, tidak perlu dilaporkan
126.	Pasal 25 (1) Pengendali Data Pribadi wajib menghentikan pemrosesan Data Pribadi dalam hal Pemilik Data Pribadi menarik kembali persetujuan pemrosesan Data Pribadi.	Bagaimana mekanisme penarikan kembali persetujuan? Untuk penghentian pemrosesan Data Pribadi, apakah dapat menggunakan button opt out saja? berapa lama jangka waktu yang diberikan, di sini belum ada penjelasannya. Perlu disesuaikan dengan kemampuan IT Kami menyarankan untuk mengubah kerangka waktu menjadi "dalam jumlah waktu yang wajar dengan menyesuaikan keadaan yang berlaku"
127.	(2) Penghentian pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) dilakukan paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak Pengendali Data Pribadi menerima permintaan penarikan kembali persetujuan pemrosesan Data Pribadi.	Untuk waktu apakah bisa diberikan Jangka waktu ini terlalu restriktif kami mengusulkan agar dapat diubah menjadi paling lambat 1 bulan sesuai dengan *international best practice* (termasuk GDPR). Selain itu, menurut hemat kami tidak semua Pengendali Data Pribadi mempunyai sistem dan/atau SDM yang mencukupi untuk melakukan hal tersebut. GDPR memberikan waktu **satu bulan sejak permohonan diterima,** dan **dapat diperpanjang dua bulan.** Sedangkan, PDPA Malaysia memberikan waktu 21 hari (dan dapat diperpanjang). **Masukan:** Disamakan dengan GDPR/ PDPA Malaysia
128.	Pasal 26 (1) Pengendali Data Pribadi wajib melakukan penundaan dan pembatasan pemrosesan Data Pribadi baik sebagian atau seluruhnya paling lambat 2 x 24 (dua kali dua puluh empat) jam terhitung sejak Pengendali Data Pribadi menerima permintaan penundaan dan pembatasan pemrosesan Data Pribadi.	Hal ini akan menyulitkan Pengendali Data Pribadi karena bagaimana menginformasikan kepada pemilik data pribadi terkait pergerakan datanya sehingga pemilik data pribadi mengetahui dimana pemrosesan data pribadi. Jika dilakukan maka akan memberitahu kepada pemilik data

		pribadi proses pemrosesan milik Pengendali Data Pribadi yang mana hal tersebut bersifat confidential. Jangka waktu ini terlalu restriktif kami mengusulkan agar dapat diubah menjadi paling lambat 1 bulan sesuai dengan *international best practice* (termasuk GDPR). Selain itu, menurut hemat kami tidak semua Pengendali Data Pribadi mempunyai sistem dan/atau SDM yang mencukupi untuk melakukan hal tersebut. GDPR memberikan waktu **satu bulan sejak permohonan diterima,** dan **dapat diperpanjang dua bulan.** Sedangkan, PDPA Malaysia memberikan waktu 21 hari (dan dapat diperpanjang). **Masukan:** Disamakan dengan GDPR/ PDPA Malaysia
129.	(2) Penundaan dan pembatasan pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) dikecualikan dalam hal:	Apakah hal ini dimaksud dengan persetujuan? Apakah diperbolehkan di dalam perjanjian dengan Pengendali Data jika disampaikan bahwa Pemilik Data Pribadi tidak boleh mengajukan Penundaan dan pembatasan pemrosesan?
130.	a. terdapat ketentuan peraturan perundang-undangan yang tidak memungkinkan dilakukan penundaan dan pembatasan pemrosesan Data Pribadi;	
131.	b. dapat membahayakan keselamatan pihak lain; dan/atau	
132.	c. Pemilik Data Pribadi terikat perjanjian tertulis dengan Pengendali Data Pribadi yang tidak memungkinkan dilakukan penundaan dan pembatasan pemrosesan Data Pribadi.	Diusulkan untuk dihapus atau terdapat kewajiban secara general. Pengendali data dapat memaksakan kehendak. Pemilik data pribadi adalah pemutus akhir.
133.	Pasal 27 Pengendali Data Pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya, dengan melakukan:	

134.	a. penyusunan dan penerapan langkah teknis operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan; dan	Perlu adanya panduan dari Kominfo untuk pelaksanaan teknisnya agar memiliki arahan yang sama untuk seluruh pengendali data Kami merekomendasikan untuk mengubah Pasal 27a menjadi sebagai berikut: "Personal Data Controller harus melindungi dan memastikan keamanan Data Pribadi yang dimilikinya atau di bawah kendalinya dengan membuat pengaturan keamanan yang wajar untuk mencegah akses, pengumpulan, penggunaan, pengungkapan, penyalinan, modifikasi, pembuangan, atau risiko serupa yang tidak sah."
135.	b. penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi.	Perlu adanya panduan dari Kominfo untuk pelaksanaan teknisnya agar memiliki arahan yang sama untuk seluruh pengendali data
136.	Pasal 28 Pengendali Data Pribadi wajib melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan Data Pribadi di bawah kendali Pengendali Data Pribadi.	Bagaimana bentuk pengawasannya? Perlu untuk dijelaskan lebih lanjut bentuk pengawasan yang wajib dilakukan.
137.	Pasal 29 Pengendali Data Pribadi wajib memastikan pelindungan Data Pribadi dari pemrosesan Data Pribadi yang tidak sah.	Bentuk tata caranya seperti apa? mohon dijelaskan lebih terperinci untuk hal ini agar seluruh pengendali data dapat memiliki arahan yang sama mengenai batasan keabsahan atas pemrosesan Data Pribadi oleh Pengendali Data Pribadi.
138.	Pasal 30 (1) Pengendali Data Pribadi wajib mencegah Data Pribadi diakses secara tidak sah.	

139.	(2) Pencegahan sebagaimana dimaksud pada ayat (1) dilakukan dengan menggunakan sistem keamanan terhadap Data Pribadi yang diprosesnya dan/atau memproses Data Pribadi menggunakan sistem elektronik secara andal, aman, dan bertanggung jawab.	Apa definisi sistem elektronik secara andal, aman, dan bertanggung jawab? apakah perlu sertifikasi dari lembaga yang terakreditasi?
140.	(3) Pencegahan sebagaimana dimaksud pada ayat (2) dilakukan sesuai dengan ketentuan peraturan perundang-undangan.	Dalam hal belum terdapat peraturan perundang-undangan yang mengatur mengenai hal ini, maka perlu untuk dijelaskan lebih lanjut mengenai standar pencegahan pengaksesan Data Pribadi secara tidak sah.
141.	Pasal 31 Pengendali Data Pribadi wajib melakukan perekaman terhadap seluruh kegiatan pemrosesan Data Pribadi.	Mohon penjelasan bentuk perekaman yang dimaksud, apakah berbentuk laporan, pencatatan atau lainnya. Kami merekomendasikan untuk mengubah Pasal 31 menjadi sebagai berikut: “Setiap Pengendali Data Pribadi harus memelihara catatan yang cukup menggambarkan sistem pemrosesan datanya, dan mengidentifikasi tugas dan tanggung jawab individu yang akan memiliki akses ke data pribadi. Catatan harus mencakup: Sebuah. Informasi tentang tujuan pemrosesan data pribadi, termasuk pemrosesan yang akan datang atau pembagian data; b. Deskripsi kategori umum dari subjek data, data pribadi, dan penerima data pribadi yang akan terlibat dalam pemrosesan. c. Informasi umum tentang aliran data dalam organisasi, mulai dari waktu pengumpulan, pemrosesan, dan penyimpanan, termasuk batas waktu untuk pembuangan atau penghapusan data pribadi. "
142.	Pasal 32 (1) Pengendali Data Pribadi wajib memberikan akses kepada Pemilik Data Pribadi terhadap Data Pribadi yang diproses beserta rekam jejak pemrosesan Data Pribadi sesuai dengan jangka waktu penyimpanan Data Pribadi.	Perlu diatur lebih lanjut mengenai akses yang dapat diberikan kepada pemilik data. Dalam hal ini, apakah, informasi profil dan transaksi yang dapat dilihat pada platform dapat memadai.

		Terkait jangka waktu penyimpanan, apakah Data Pribadi ini akan diselaraskan dengan jangka waktu sebagaimana tercantum dalam Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan. atau Kami merekomendasikan menghapus Pasal 32 secara keseluruhan.
143.	(2) Akses sebagaimana dimaksud pada ayat (1) diberikan paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak Pengendali Data Pribadi menerima permintaan akses.	(Jangka waktu ini terlalu restriktif kami mengusulkan agar dapat diubah menjadi paling lambat 1 bulan sesuai dengan *international best practice* (termasuk GDPR). Selain itu, menurut hemat kami tidak semua Pengendali Data Pribadi mempunyai sistem dan/atau SDM yang mencukupi untuk melakukan hal tersebut. GDPR memberikan waktu **satu bulan sejak permohonan diterima,** dan **dapat diperpanjang dua bulan.** Sedangkan, PDPA Malaysia memberikan waktu 21 hari (dan dapat diperpanjang). **Masukan:** Disamakan dengan GDPR/ PDPA Malaysia
144.	Pasal 33 Pengendali Data Pribadi wajib menolak memberikan akses perubahan terhadap Data Pribadi kepada Pemilik Data Pribadi dalam hal diketahui atau sepatutnya diduga:	Dalam hal dapat mendefinisikan “sepatutnya diduga” bagaimana pembuktiannya? Diusulkan untuk ditambahkan poin (d) Tidak dapat divalidasi / diverifikasi sesuai dengan hukum, medis atau dokumentasi lain yang relevan yang tersedia untuk Pengendali Data Pribadi
145.	a. membahayakan keamanan atau kesehatan fisik atau kesehatan mental Pemilik Data Pribadi dan/atau orang lain;	Perlu diatur mengenai mekanisme verifikasi atas kesehatan fisik atau kesehatan mental Pemilik Data Pribadi, mengingat hal ini sulit untuk diidentifikasi oleh Pemilik Data Pribadi.
146.	b. berdampak pada pengungkapan Data Pribadi milik orang lain; dan/atau	

147.	c. bertentangan dengan kepentingan pertahanan dan keamanan nasional.	Dalam Pasal ini perlu ditambahkan klausa berupa huruf d yang menyatakan ***"Jika melanggar peraturan perundang-undangan".***
148.	Pasal 34 (1) Pengendali Data Pribadi wajib memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi paling lambat 1 x 24 (satu kali dua puluh empat) jam terhitung sejak Pengendali Data Pribadi menerima permintaan pembaruan dan/atau perbaikan Data Pribadi.	Banyaknya laporan yang dapat menjadi masalah, dimana permintaan karena kegagalan pelindungan data menyebabkan banyaknya panggilan masuk, langkah-langkah berikut perlu dilakukan: • Penjelasan tentang kapan periode pemberitahuan dimulai (misal seharusnya berdasarkan pengetahuan dan bukan pada saat terjadinya - yang tidak secara khusus dinyatakan dalam RUU ini). • Berdasarkan GDPR pemberitahuan hanya diperlukan jika pelanggaran data cenderung "mengakibatkan risiko hak dan kebebasan individu atau dalam bahaya signifikan terhadap pemilik data pribadi.". Meskipun ini juga bisa subjektif, setidaknya pemberitahuan tidak berlaku untuk setiap pelanggaran. Perlu menambahkan kondisi serupa dalam RUU ini. • Selain itu, pendekatan pemberitahuan disampaikan pada Komisi dan pemilik data, dimana pemrosesan atau akses yang tidak sah telah terjadi (mis. Pelanggaran telah dikonfirmasi) yang kemungkinan akan mengakibatkan kerusakan materi yang signifikan terhadap pemilik data. • Seharusnya ada ambang batas yang jelas untuk pemberitahuan pelanggaran data. Ambang yang tidak jelas akan menyebabkan ketidakpastian dan beban yang tidak perlu bagi para regulator dan bisnis. • Menerapkan konsep batasa dan ketegori "bahaya signifikan" atau "bahaya serius" terhadap pelanggaran pemberitahuan dapat

		membantu memastikan regulator memiliki visibilitas ke dalam insiden yang menimbulkan risiko sesungguhnya bagi pengguna dan memastikan regulator dapat memfokuskan kegiatan pembinaan dan pengawasan dimana mereka paling dibutuhkan . • Namun, jika ambang atas 'bahaya' terlalu rendah, hal ini dapat mengakibatkan munculnya notifikasi secara berlebihan kepada regulator dan individu. Selai itu hal ini juga untuk memberikan lebih banyak kepastian kepada agensi dan untuk lebih menyelaraskan dengan negara lain yang memiliki ambang batas lebih tinggi ketika pelanggaran privasi seharusnya diberitahukan Jangka waktu yang diusulkan sangat singkat. Penting untuk mempertimbangkan bahwa penilaian tentang apakah permintaan pemilik data dapat diterima dan penilaian yang sesuai untuk mengonfirmasi apakah pengecualian berlaku memerlukan waktu. Hal ini juga ini tidak akan praktis dalam hal pemrosesan data oleh perusahaan multinasional global dengan jumlah data yang besar. RUU ini seharusnya meniadakan referensi waktu dan mengatur sesuatu yang lebih praktis dengan "sesegera mungkin secara praktis/tanpa penundaan yang tidak semestinya", atau memperpanjang tenggat waktu untuk menunda atau membatasi operasi pemrosesan menjadi kerangka waktu yang lebih masuk akal dalam waktu 30 hari sesuai dengan *international best practice* (termasuk GDPR). Selain itu, menurut hemat kami tidak semua Pengendali Data Pribadi mempunyai

		sistem dan/atau SDM yang mencukupi untuk melakukan hal tersebut. GDPR memberikan waktu **satu bulan sejak permohonan diterima,** dan **dapat diperpanjang dua bulan.** Sedangkan, PDPA Malaysia memberikan waktu 21 hari (dan dapat diperpanjang). **Masukan:** Disamakan dengan GDPR/ PDPA Malaysia
149.	(2) Pengendali Data Pribadi wajib memberitahukan hasil pembaruan dan/atau perbaikan Data Pribadi kepada Pemilik Data Pribadi.	
150.	Pasal 35 (1) Pengendali Data Pribadi wajib menjamin akurasi, kelengkapan, dan konsistensi Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan.	Beberapa pertanyaan mengenai pasal ini 1. Apa yang dimaksud dengan akurasi, kelengkapan, dan konsistensi? 2. Apakah verifikasi yang dimaksud di sini? 3. Mengapa Pengendali Data Pribadi wajib melakukan verifikasi? 4. Bagaimana dengan bidang usaha yang tidak memerlukan keakuratan Data untuk dapat memberikan layanannya tetapi perlu untuk mengumpulkan Data Pribadi? 5. apakah kewajiban ini merupakan kewajiban dari si pemilik data? 6. pelaku usaha dapat meminta konfirmasi secara berkala tapi itu adalah tanggung jawab dari pemilik data pribadi Dari sisi akurasi, menurut hemat kami sulit bagi Pengendali Data Pribadi untuk dapat menjamin akurasi, kelengkapan dan konsistensi Data Pribadi. Menurut hemat kami, hal ini merupakan kewajiban Pemilik Data Pribadi selaku pihak yang mempunyai kewenangan

		untuk memberikan Data Pribadi kepada Pengendali Data Pribadi. Selain itu, kewajiban ini melebar dari definisi Pengendali Data Pribadi.
151.	(2) Dalam menjamin akurasi, kelengkapan, dan konsistensi Data Pribadi sebagaimana dimaksud pada ayat (1) Pengendali Data Pribadi wajib melakukan verifikasi.	
152.	Pasal 36 Pengendali Data Pribadi wajib melakukan pemrosesan Data Pribadi sesuai dengan tujuan pemrosesan Data Pribadi yang disetujui oleh Pemilik Data Pribadi.	
153.	Pasal 37 (1) Pengendali Data Pribadi wajib mengakhiri pemrosesan Data Pribadi jika:	Berdasarkan PP 80 tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, masa retensi paling singkat 10 tahun, apakah Pengendali Data Pribadi dapat menentukan sendiri masa retensinya dengan batasan paling singkat 10 tahun? Masukan untuk Memberlakukan Pengecualian (1) Jika diminta untuk mematuhi hukum dan peraturan (2) Anti Pencucian Uang dan Pendanaan Penanggulangan Terorisme (3) Pencegahan Penipuan
154.	a. telah mencapai masa retensi;	Batas waktu retensi dimasukkan agar lebih jelas. Apakah Data Pribadi ini akan diselaraskan dengan jangka waktu sebagaimana tercantum dalam Undang-undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan.
155.	b. tujuan pemrosesan Data Pribadi telah tercapai; atau	
156.	c. terdapat permintaan dari Pemilik Data Pribadi.	
157.	(2) Pengakhiran pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) dilakukan sesuai dengan ketentuan peraturan perundangundangan.	

158.	Pasal 38 (1) Pengendali Data Pribadi wajib menghapus Data Pribadi jika:	Beberapa hal yang perlu diklarifikasi: • Apabila Data Pribadi masih dapat dipulihkan atau ditampilkan, apakah artinya Pengendali Data masih harus menyimpan Data Pribadi setelah dihapus? • Apakah Pengendali dapat melakukan proses anonym terhadap Data Pribadi yang telah melewati masa retensinya sesuai dengan kepentingan sahnya (Pasal 18 (2) f.)? • Dengan adanya RUU PDP apakah mekanisme penghapusan dengan penetapan pengadilan tersebut masih diacu? karena RUU PDP mengacu kepada peraturan perundang-undangan yang berlaku, sedangkan terdapat asas hukum bahwa peraturan yang baru mengesampingkan peraturan yang lama (Lex posterior derogat legi priori). Oleh karena itu, seharusnya RUU PDP memberi penegasan mekanisme penghapusannya lebih jelas, apakah masih seperti UU ITE. • Perihal tindakan penghapusan Data Pribadi oleh Pengendali perlu diperjelas, apakah penghapusan cukup dengan menghilangkannya dari tampilan, tetapi Pengendali tetap berhak untuk menyimpan data? Karena pada RUU PDP dimungkinkan agar “data dipulihkan”. Artinya, pada saat Pemilik meminta data dihapus, Pengendali cukup menghilangkan dari penampilan dan pada saat Pemilik meminta dipulihkan, Pengendali dapat langsung menampilkan.

		• perlu adanya aturan yang mengatur lebih jelas mengenai penghapusan data, dan penarikan kembali data pribadi oleh pemilik data. Sebagai contoh pada Penyelenggara LPMUBTI*:* apabila pada saat pemilik data pribadi telah mengajukan aplikasi dan memberikan data pribadi untuk diproses oleh Penyelenggara, dan data telah masuk dalam tahap pemrosesan oleh Penyelenggara, maka pemilik data pribadi tidak bisa secara langsung atau serta-merta melakukan penarikan data pada saat proses tersebut secara sepihak. Karena terdapat beberapa dampak terhadap Penyelenggara dalam memberikan Layanannya, seperti: Penyelenggara lalai dalam pembuktian rekam jejak audit kepada regulator/pengawas, sebagaimana diatur dalam peraturan perundang-undangan terkait; dan Menghambat efektivitas dan efisiensi biaya yang telah dikeluarkan Penyelenggara dalam hal pelaksanaan proses data pribadi tersebut. Untuk itu kami memberikan masukan 1. Memberlakukan Pengecualian - Jika diminta untuk mematuhi hukum dan peraturan - Anti Pencucian Uang dan Pendanaan Penanggulangan Terorisme - Pencegahan Penipuan 2.Merekomendasikan untuk mengklarifikasi perbedaan antara "penghancuran" data pribadi

		berdasarkan Pasal ini dan "penghapusan" data pribadi berdasarkan Pasal 38. Sejauh hal itu berarti hal yang sama, kami sarankan untuk menggabungkan dan merampingkan Pasal 38 dan 39.
159.	a. Data Pribadi tidak lagi diperlukan untuk pencapaian tujuan pemrosesan Data Pribadi;	
160.	b. Pemilik Data Pribadi telah melakukan penarikan kembali persetujuan pemrosesan Data Pribadi;	Dalam hal tidak ada lagi kewajiban yang timbul karena kesepakatan Para Pihak yang timbul sebelum Penarikan dilakukan
161.	c. terdapat permintaan dari Pemilik Data Pribadi; atau	
162.	d. Data Pribadi diperoleh dan/atau diproses dengan cara melawan hukum.	
163.	(2) Penghapusan Data Pribadi sebagaimana dimaksud pada ayat (1) dilakukan sesuai dengan ketentuan peraturan perundang-undangan.	
164.	(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.	Pasal ini diusulkan untuk dihapus atau diberikan penjelasan sebagai berikut • Apabila Data Pribadi masih dapat dipulihkan atau ditampilkan, apakah artinya Pengendali Data masih harus menyimpan Data Pribadi setelah dihapus? • Apakah Pengendali dapat melakukan proses anonym terhadap Data Pribadi yang telah melewati masa retensinya sesuai dengan kepentingan sahnya (Pasal 18 (2) f.)? • Apakah artinya data yang dihapus tapi masih dalam masa retensi tidak boleh benar-benar dihapus?
165.	(4) Permintaan sebagaimana dimaksud pada ayat (3) dapat diajukan dalam hal belum melewati masa retensi sesuai dengan ketentuan peraturan perundang-undangan.	Bagaimana ketentuan Masa Retensi Data Pribadi? Mengusulkan untuk batas waktu retensi dimasukkan agar lebih jelas
166.	Pasal 39 (1) Pengendali Data Pribadi wajib memusnahkan Data Pribadi jika:	Hal ini menyulitkan model bisnis yang berbasis pemrosesaan data seperti marketplace yang basisnya adalah pemrosesan data. Kewajiba ini juga

		terlalu strict pada bebereapa kegiatan usaha seperti marketplace. Mengusulkan untuk Memberlakukan Pengecualian (1) Jika diminta untuk mematuhi hukum dan peraturan (2) Anti Pencucian Uang dan Pendanaan Penanggulangan Terorisme (3) Pencegahan Penipuan Kami merekomendasikan untuk mengklarifikasi perbedaan antara "penghancuran" data pribadi berdasarkan Pasal ini dan "penghapusan" data pribadi berdasarkan Pasal 38. Sejauh hal itu berarti hal yang sama, kami sarankan untuk menggabungkan dan merampingkan Pasal 38 dan 39.
167.	a. tidak memiliki nilai guna lagi;	
168.	b. telah habis masa retensinya dan berketerangan dimusnahkan berdasarkan jadwal retensi arsip;	Batas waktu retensi dimasukkan agar lebih jelas
169.	c. terdapat permintaan dari Pemilik Data Pribadi; atau	
170.	d. tidak berkaitan dengan penyelesaian proses hukum suatu perkara.	
171.	(2) Pemusnahan Data Pribadi sebagaimana dimaksud pada ayat (1) dilakukan sesuai dengan ketentuan peraturan perundang-undangan.	
172.	Pasal 40 (1) 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:	Beberapa hal yang perlu diklarifikasi: • apabila kebocoran tersebut terjadi di partner pengendali data pribadi, apakah pengendali data pribadi juga tanggung renteng bertanggung jawab dan memberikan pelaporan atas kegagalan pelindungan data pribadi?

		• Pemberitahuan tertulis sejak diketahuinya terjadi kebocoran data? • Apa yang dimaksud dengan kegagalan pelindungan Data Pribadi? • Mohon penjelasan terkait definisi daripada kegagalan perlindungan Data Pribadi dan lebih terukur apa yang harus dilaporkan. Misalnya apakah hanya 1 data bocor menyebabkan kewajiban pelaporan? Untuk itu kami memberi masukan • Batasan definisi yang terukur atas jumlah Data Pribadi yang bocor sehingga kewajiban atas pelaporan tersebut timbul.Lebih lanjut, kami menyarankan agar diberikan waktu lebih lama juga untuk penyampaian pelaporan dan diperjelas jangka waktu ini apakah dimulai setelah pelaku usaha sadar akan terjadinya kebocoran atau setelah kejadian itu sendiri muncul. • memasukkan ketentuan yang lebih jelas tentang apa yang dianggap sebagai kegagalan untuk melindungi data pribadi dan ambang batas untuk pelanggaran data, khususnya yang perlu dibuat tersedia untuk umum. • Perlu diatur secara jelas mengenai titik tolak waktu penyampaian pemberitahuan secara tertulis, diusulkan untuk diatur titik tolaknya semenjak Pengendali Data Pribadi mengetahui adanya kegagalan pelindungan Data Pribadi.

		Perbedaan jangka waktu pemberitahuan kegagalan perlindungan Data Pribadi yang lebih singkat di dalam RUU PDP dibandingkan Permenkominfo Nomor 20/2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (14 hari) akan membutuhkan penyesuaian signifikan. Disamping itu, walaupun pasal ini merujuk pada prinsip *without undue delay*, akan tetapi perlu dipertimbangkan bahwa tingkat dan kapasitas Pengendali Data Pribadi sangat beragam di Indonesia. Tidak semua Pengendali Data Pribadi dapat memenuhi kewajiban ini dalam waktu yang singkat, terutama apabila kegagalan diakibatkan oleh pihak eksternal yang memerlukan investigasi forensik.
173.	a. Pemilik Data Pribadi; dan	
174.	b. Menteri.	
175.	(2) Pemberitahuan tertulis sebagaimana dimaksud pada ayat (1) mengenai:	
176.	a. Data Pribadi yang terungkap;	Yang terungkap atau diungkapkan tanpa adanya bentuk non disclosure agreement
177.	b. kapan dan bagaimana Data Pribadi terungkap; dan	Bagaimana jika Pengendali data pribadi tidak tau data itu milik siapa dan data tersebut tidak dapat diidentifikasi siapa pemilik datanya?
178.	c. upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi.	
179.	(3) Dalam hal tertentu Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan pelindungan Data Pribadi.	

180.	Pasal 41 Pengendali Data Pribadi wajib bertanggung jawab atas pemrosesan Data Pribadi dan menunjukkan pertanggungjawabannya dalam pemenuhan kewajiban pelaksanaan prinsip pelindungan Data Pribadi.	
181.	Pasal 42 (1) Kewajiban Pengendali Data Pribadi sebagaimana dimaksud dalam Pasal 32, Pasal 34, Pasal 37, Pasal 38 ayat (1) huruf a, huruf b, dan huruf c, Pasal 39 ayat (1) huruf c, dan Pasal 40 ayat (1) huruf a, tidak berlaku untuk:	Bagaimana masyarakat dapat mengetahui bahwa tidak terjadi penyalahgunaan dan/atau kegagalan perlindungan Data Pribadi dalam hal Pengendali menjalankan kepentingan-kepentingan tersebut?
182.	a. kepentingan pertahanan dan keamanan nasional;	
183.	b. kepentingan proses penegakan hukum;	
184.	c. kepentingan umum dalam rangka penyelenggaraan negara;	
185.	d. kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan; atau	
186.	e. agregat data yang pemrosesannya ditujukan guna kepentingan statistik dan penelitian ilmiah dalam rangka penyelenggaraan negara.	Agar kalimat “yang pemrosesannya ditujukan guna kepentingan statistik dan penelitian ilmiah dalam rangka penyelenggaraan negara” dihapuskan dari Pasal 42 ayat 1 huruf e Pasal 1 ayat 1 RUU PDP menyebutkan Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik. Berdasarkan definisi tersebut data agregat bukan merupakan data pribadi karena data agregat bukan merupakan data tentang seseorang, sehingga pengunaannya tidak perlu dibatasi. Pembatasan pemrosesan data agregat tidak membawa manfaat terhadap PDP

		tetapi justru dapat menghambat pertumbuhan industri digital.
187.	(2) Pengecualian sebagaimana dimaksud pada ayat (1) dilaksanakan hanya dalam rangka pelaksanaan ketentuan Undang-Undang.	
188.	Bagian Ketiga Kewajiban Prosesor Data Pribadi	
189.	Pasal 43 (1) Dalam hal Pengendali Data Pribadi menunjuk Prosesor Data Pribadi, Prosesor Data Pribadi wajib melakukan pemrosesan Data Pribadi berdasarkan instruksi atau perintah Pengendali Data Pribadi kecuali ditentukan lain berdasarkan ketentuan peraturan perundang-undangan.	mendukung pendekatan Indonesia antara tanggung jawab Personal Data Controller dan Personal Data Processor, sebagaimana diuraikan dalam Pasal 43 Rancangan Undang-Undang. Namun, Pasal 44 membingungkan karena menyebutkan kewajiban-kewajiban yang diberikan kepada para Personal Data Controller dan bukan pada Personal Data Processor. Terutama kewajiban-kewajiban berikut ini yang harus dialamatkan kepada para Personal Data Controller dan *bukan* Personal Data Processor: (i) Pasal 27 tentang Personal Data Controller melindungi dan memastikan keamanan data pribadi; (ii) Pasal 28 tentang Personal Data Controller mengawasi Personal Data Processor; (iii) Pasal 29 tentang Personal Data Controller memastikan perlindungan data dari pemrosesan yang tidak valid; (iv) Pasal 30 tentang Personal Data Controller mencegah akses ilegal; (v) Pasal 31 tentang Personal Data Controller menyimpan catatan; dan (vi) Pasal 35 tentang Personal Data Controller menjamin keakuratan, kelengkapan, dan konsistensi data pribadi. Personal Data Processor seringnya tidak melihat secara langsung data customer mereka dan tidak akan mampu menentukan apakah suatu data pribadi sedang diproses, dan oleh karena itu,

		tidak wajar untuk diharapkan untuk mengetahui kapan dan apakah mereka harus melakukan pemrosesan untuk memenuhi kewajiban PDP. Seharusnya, Personal Data Processor diharapkan untuk menerapkan langkah-langkah keamanan yang wajar dan sesuai untuk Sistem Elektronik mereka. Karena itu, kami menyarankan agar Pasal 44 dihapus secara keseluruhan. Dan sebagai gantinya, Pemerintah Indonesia dapat mempertimbangkan mengubah Pasal 43 dengan memasukkan bahasa yang serupa dalam Pasal 21(1) tentang kerahasiaan, dan tanggung jawab seorang Personal Data Processor untuk menerapkan standard teknis dan organisasi yang sesuai atas instruksi dari Personal Data Controller.
190.	(2) Pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1), dilaksanakan dengan memperhatikan ketentuan pemrosesan Data Pribadi berdasarkan Undang-Undang ini.	
191.	(3) Pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) termasuk dalam tanggung jawab Pengendali Data Pribadi.	
192.	(4) Dalam hal Prosesor Data Pribadi melakukan pemrosesan Data Pribadi diluar instruksi atau perintah dan tujuan yang ditetapkan Pengendali Data Pribadi, pemrosesan Data Pribadi menjadi tanggung jawab Prosesor Data Pribadi.	
193.	Pasal 44 Kewajiban sebagaimana dimaksud dalam Pasal 21 ayat (1), Pasal 27, Pasal 28, Pasal 29, Pasal 30, Pasal 31, dan Pasal 35 berlaku juga terhadap Prosesor Data Pribadi.	
194.	Bagian Keempat Pejabat atau Petugas Yang Melaksanakan Fungsi Pelindungan Data Pribadi	

195.	Pasal 45 (1) Dalam hal tertentu Pengendali Data Pribadi dan Prosesor Data Pribadi wajib menunjuk seorang pejabat atau petugas yang melaksanakan fungsi pelindungan Data Pribadi.	Secara teknis, kami juga menyarankan agar lebih lanjut diatur tentang: a. Siapa dari perusahaan yang dapat memegang peran ini? b. Standar kualifikasi teknis apa saja yang harus dimiliki Petugas yang melaksanakan fungsi Pelindungan Data Pribadi yang dimiliki perusahaan?
196.	(2) Dalam hal tertentu sebagaimana dimaksud pada ayat (1) meliputi:	Apa yang menjadi indicator skala besar? Apakah yang dimaksud dengan “pelayanan publik” pada ketentuan ini
197.	a. pemrosesan Data Pribadi untuk kepentingan pelayanan publik;	Ketentuan dalam GDPR yang diterjemahkan untuk poin ini adalah sebagai berikut: Art 37 (1)(a): “***The controller and the processor shall designate a data protection officer in any case where the processing is carried out by a public authority or body, except for courts acting in their judicial capacity***” *The Article 29 Data Protection Working Party* kemudian memberikan penjelasan yang dimaksud dengan "*public authority or body*" adalah: • Badan publik termasuk otoritas baik di tingkat pusat maupun daerah, namun secara konseptual, berdasarkan hukum yang berlaku, juga mencakup lembaga-lembaga yang diatur dalam hukum publik; atau • Pihak yang bukan merupakan badan publik dan diatur dalam hukum privat (misal UU perseroan terbatas) yang menjalankan fungsi pelayanan publik (*public task*) atau kewenangan publik (*public authority*) dalam sektor-sektor seperti transportasi umum, penyediaan air dan listrik, jalanan, perumahan rakyat atau penyiaran publik.

		Penjelasan ini perlu juga dimasukkan dalam RUU PDP. Makna dari "**kepentingan publik**" sangat luas dan tidak ada tolak ukurnya, sehingga perlu dijelaskan untuk menciptakan kepastian hukum bagi pelaksanaan perlindungan data pribadi di Indonesia.
198.	b. kegiatan inti Pengendali Data Pribadi memiliki sifat, ruang lingkup, dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas Data Pribadi dengan skala besar; dan	Ketentuan pada poin ini menerjemahkan ketentuan dari GDPR sebagai berikut: Article 37 (1)(b): "***the core activities of the [parties that collect/process personal data] consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale***" Menurut kami, pasal ini apabila dimaknai bahwa kewajiban untuk menunjuk fungsi perlindungan data pribadi dalam perusahaan apabila kegiatan utama dari **pihak yang mengumpulkan atau memroses data pribadi** terdiri dari aktivitas pemrosesan yang berdasarkan sifat, ruang lingkup dan/atau tujuan dari pemrosesan tersebut **memerlukan pemantauan subyek data yang dilakukan secara sistematis, rutin dan dalam skala besar**. Sistematis, rutin dan skala besar di sini harus diberikan tolak ukur karena tidak jelas dalam implementasinya bagaimanakah yang disebut sistematis, rutin dan skala besar. GDPR memang tidak mendefinisikan lebih lanjut mengenai frasa tersebut, namun *The Article 29 Data Protection Working Party* memberikan penjelasan mengenai persyaratan penunjukan fungsi perlindungan data pribadi dalam perusahaan, yaitu sebagai berikut: • pemrosesan dalam skala besar dapat dipertimbangkan berdasarkan faktor-faktor sebagai berikut: (i) jumlah pemilik data pribadi yang

		dikumpulkan/diproses, (ii) jumlah dan/atau macam-macam data yang dikumpulkan/diproses, (iii) durasi pemrosesan data pribadi atau (iv) besaran wilayah yang dijadikan objek dari kegiatan pengumpulan/pemrosesan data; • Yang dimaksud dengan "rutin" adalah (i) terjadi pada suatu interval dan dalam waktu tertentu, (ii) berlangsung berulang kali pada waktu tertentu atau (iii) terjadi secara konstan atau dari waktu ke waktu (periodically); • "**sistematis**" dapat diartikan: (i) terjadi berdasarkan suatu sistem, (ii) terorganisir atau berdasarkan suatu metode tertentu, (iii) berlangsung karena merupakan bagian dari suatu rencana pengumpulan/pemrosesan data pribadi lain atau (iv) dilakukan sebagai bagian dari suatu strategi. Tolak ukur ini perlu dimasukkan dalam RUU PDP.
199.	c. kegiatan inti Pengendali Data Pribadi terdiri dari pemrosesan Data Pribadi dalam skala besar untuk Data Pribadi yang bersifat spesifik dan/atau Data Pribadi yang berkaitan dengan tindak pidana.	Skala besar untuk poin ini juga harap diberikan tolak ukur dalam RUU PDP.
200.	(3) Pejabat atau petugas yang melaksanakan fungsi pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) harus ditunjuk berdasarkan kualitas profesional, pengetahuan mengenai hukum dan praktik pelindungan Data Pribadi, dan kemampuan untuk memenuhi tugas-tugasnya.	
201.	(4) Pejabat atau petugas yang melaksanakan fungsi pelindungan Data Pribadi sebagaimana dimaksud pada ayat (3) dapat berasal dari dalam dan/atau luar Pengendali Data Pribadi atau Prosesor Data Pribadi.	Mohon penjelasan apakah yang dimaksud dengan dari luar Pengendali Data Pribadi atau Prosesor Data Pribadi dapat juga mencakup konsultan atau pihak lain yang bukan merupakan karyawan dari Pengendali Data Pribadi.

		apakah maksudnya indepen? apakah perlu ada sertifikat khusus yang dimilki data officer tersebut?
202.	Pasal 46 (1) Pejabat atau petugas yang melaksanakan fungsi pelindungan Data Pribadi memiliki tugas paling sedikit:	
203.	a. menginformasikan dan memberikan saran untuk Pengendali Data Pribadi atau Prosesor Data Pribadi agar mematuhi ketentuan dalam Undang-Undang ini;	
204.	b. memantau dan memastikan kepatuhan terhadap Undang-Undang ini dan kebijakan Pengendali Data Pribadi atau Prosesor Data Pribadi, termasuk penugasan, tanggung jawab, peningkatan kesadaran dan pelatihan pihak yang terlibat dalam pemrosesan Data Pribadi, dan audit terkait;	
205.	c. memberikan saran mengenai penilaian dampak pelindungan Data Pribadi dan memantau kinerja Pengendali Data Pribadi dan Prosesor Data Pribadi; dan	
206.	d. berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan Data Pribadi, termasuk melakukan konsultasi mengenai mitigasi risiko dan/atau hal lainnya.	
207.	(2) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), pejabat atau petugas yang melaksanakan fungsi pelindungan Data Pribadi memperhatikan risiko terkait pemrosesan Data Pribadi, dengan mempertimbangkan sifat, ruang lingkup, konteks, dan tujuan pemrosesan.	
208.	(3) Ketentuan lebih lanjut mengenai pejabat atau petugas yang melaksanakan fungsi pelindungan Data Pribadi diatur dalam Peraturan Pemerintah.	
209.	BAB VI TRANSFER DATA PRIBADI	
210.	Bagian Kesatu Transfer Data Pribadi Dalam Wilayah Hukum Negara Kesatuan Republik Indonesia	

211.	Pasal 47 (1) Pengendali Data Pribadi dapat mentransfer Data Pribadi kepada Pengendali Data Pribadi lainnya dalam wilayah hukum Negara Kesatuan Republik Indonesia.	
212.	(2) Pengendali Data Pribadi yang mentransfer Data Pribadi dan yang menerima transfer Data Pribadi wajib melakukan pelindungan Data Pribadi sebagaimana dimaksud dalam Undang-Undang ini.	Masukan untuk menambahkan ketentuan agar transfer data pribadi dilakukan sesuai dengan suatu standar keamanan IT (misalnya harus terenkripsi, dll)
213.	Pasal 48 (1) Pengendali Data Pribadi berbentuk badan hukum yang melakukan penggabungan, pemisahan, pengambilalihan, atau peleburan badan hukum wajib menyampaikan pemberitahuan pengalihan Data Pribadi kepada Pemilik Data Pribadi.	
214.	(2) Pemberitahuan pengalihan Data Pribadi sebagaimana dimaksud pada ayat (1) dilakukan sebelum dan sesudah penggabungan, pemisahan, pengambilalihan, atau peleburan badan hukum.	
215.	(3) Dalam hal Pengendali Data Pribadi berbentuk badan hukum melakukan pembubaran atau dibubarkan, penyimpanan, transfer, penghapusan, atau pemusnahan Data Pribadi dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.	
216.	(4) Penyimpanan, transfer, penghapusan, atau pemusnahan Data Pribadi sebagaimana dimaksud pada ayat (3) diberitahukan kepada Pemilik Data Pribadi.	Jika transfer data pribadi kepada Pihak Ketiga untuk kepentingan analisa kredit setiap saat selalu harus meminta izin, padahal sudah ada Non Disclosure Agreement maka ini akan memakan waktu SLA
217.	Bagian Kedua Transfer Data Pribadi Ke Luar Wilayah Hukum Negara Kesatuan Republik Indonesia	
218.	Pasal 49 (1) Pengendali Data Pribadi dapat mentransfer Data Pribadi kepada Pengendali Data Pribadi di luar wilayah hukum Negara Kesatuan Republik Indonesia dalam hal:	Mohon klarifikasi terkait ketentuan transfer Data Pribadi disini, dalam hal pemilik data pribadi belum menyediakan persetujuan untuk transfer, apakah dapat diartikan transfer data pribadi ke luar negeri dapat dilakukan tanpa persetujuan data pribadi, selama paling

		sedikit satu dari ketentuan dibawah terpenuhi: • negara tempat kedudukan Pengendali Data Pribadi atau organisasi internasional yang menerima transfer Data Pribadi memiliki tingkat pelindungan Data Pribadi yang setara atau lebih tinggi dari yang diatur dalam Undang-Undang ini; • terdapat perjanjian internasional antarnegara; dan/atau • terdapat kontrak antar Pengendali Data Pribadi yang memiliki standar dan/atau jaminan pelindungan data pribadi sesuai dengan yang diatur dalam Undang-Undang ini. Apabila jawabannya iya, maka apakah pasal tersebut merupakan pengecualian dari Pasal 51 (3) yang menyebutkan bahwa setiap Orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya? Apakah Kementrian Komunikasi dan Informatika akan mengeluarkan daftar negara-negara yang memenuhi ketentuan (i) di atas? Kami ingin mengusulkan untuk kondisi berikut ditambahkan ke pasal 49.1 a. Pengontrol Data telah menyediakan perlindungan yang tepat, dan dengan syarat tersedia hak subyek data dan pemulihan hukum yang efektif untuk subyek data; b. ada aturan perusahaan yang mengikat terkait perlindungan data pribadi antara anggota grup perusahaan c. transfer diperlukan untuk pelaksanaan kontrak antara subjek data dan pengontrol atau penerapan tindakan pra-

		kontraktual yang diambil atas permintaan subjek data; d. transfer diperlukan untuk kesimpulan atau kinerja kontrak yang dibuat untuk kepentingan subjek data antara pengontrol dan orang alami atau badan hukum lainnya; e. transfer diperlukan untuk alasan penting kepentingan umum; f. transfer diperlukan untuk pendirian, pelaksanaan atau pembelaan klaim hukum; g. transfer diperlukan untuk melindungi kepentingan vital subjek data atau orang lain, di mana subjek data secara fisik atau hukum tidak mampu memberikan persetujuan Dan pada Pasal 49 ayat 1 diusulkan revisi butir c dan ditambahkan 1 butir d sebagaimana dijelaskan dibawah Data merupakan sumber daya yang sangat berharga, sehingga Transfer data ke luar wilayah hukum NKRI perlu dibuat tata kelolanya untuk menjaga keseimbangan antara kedaulatan data nasional dan kemudahan berusaha untuk meningkatkan pertumbuhan ekonomi digital. Sebaiknya ketentuan pentransferan Data Pribadi ke luar wilayah Indonesia menitikberatkan pada kondisi bahwa negara tempat kedudukan Pengendali Data Pribadi atau organisasi internasional yang menerima transfer Data Pribadi memiliki tingkat perlindungan Data Pribadi yang setara atau lebih tinggi RUU PDP untuk dapat mengakomodir *data sharing* dengan memperhatikan perlindungan terbaik atas data tersebut. Selain itu, agar dapat dipertegas *data sharing* khususnya untuk kepentingan regulator terkait

		penerapan Anti Pencucian Uang dan Pendanaan Terorisme, Risiko Kredit, Pengenaan Sanksi, dsb.
219.	a. negara tempat kedudukan Pengendali Data Pribadi atau organisasi internasional yang menerima transfer Data Pribadi memiliki tingkat pelindungan Data Pribadi yang setara atau lebih tinggi dari yang diatur dalam Undang-Undang ini;	apa variabel dan indikator "memiliki tingkat pelindungan data pribadi yang setara atau lebih tinggi dari yang diatur dalam UU ini? bagaimana cara pelaku usaha menentukan dapat atau tidaknya data tersebut dikirimkan ke negara yang disyaratkan dalam pasal ini. perlu ada penjelasannya lebih lanjut.
220.	b. terdapat perjanjian internasional antarnegara;	
221.	c. terdapat kontrak antar Pengendali Data Pribadi yang memiliki standar dan/atau jaminan pelindungan data pribadi sesuai dengan yang diatur dalam Undang-Undang ini; dan/atau	Mengapa ketentuan ini menggunakan dan/atau? Diusulkan butir c diubah bunyinya menjadi: c. terdapat kontrak antar Pengendali Data Pribadi atau antara Pengendali Data Pribadi dengan Prosesor Data Pribadi yang memiliki standar dan/atau jaminan pelindungan data pribadi sesuai dengan yang diatur dalam Undang-Undang ini Kontrak dapat dilakukan antar Pengendali Data Pribadi ataupun antara Pengendali Data Pribadi Dengan Prosesor Data Pribadi oleh karena itu Pasal 49 Ayat 1 butir c diusulkan untuk ditambahkan kalimat "antara Pengendali Data Pribadi dengan Prosesor Data Pribadi" Setelah butir c diusulkan adanya penambahan butir sebagai berikut : d. teknologi pemrosesan Data Pribadi tidak atau belum tersedia di Wilayah Hukum Negara Kesatuan Republik Indonesia; Karena beberapa teknologi pemrosesan data merupakan hak paten perusahaan tertentu yang hanya dapat digunakan di

		pusat data mereka, apabila perusahaan tersebut belum membangun pusat data di Indonesia, maka Pengendali Data Pribadi yang berada di dalam wilayah hukum NKRI harus melakukan transfer Data Pribadi kepada perusahaan tersebut apabila akan melakukan kerjasama, oleh karena itu diusulkan penambahan butir d pada Pasal 49 Ayat 1
222.	d. mendapat persetujuan Pemilik Data Pribadi	Untuk lebih meningkatkan kerangka kerja, kami merekomendasikan bahwa, di samping mekanisme transfer data lintas batas dalam Pasal 49 (b, c, d), Undang-Undang harus juga secara eksplisit mencakup daftar garis besar langkah-langkah tindakan yang dapat diambil suatu entitas untuk menunjukkan bahwa mereka telah melakukan langkah-langkah yang sepatutnya, seperti: a. Personal Data Controller telah memastikan bahwa penerima data di luar negeri terikat oleh kewajiban yang sebanding berdasarkan hukum mereka yang berlaku; b. Memastikan bahwa penerima data terikat oleh peraturan korporasi yang mengikat; atau c. Memverifikasi bahwa penerima data telah memiliki sistem dan proses yang memenuhi standar yang diakui secara internasional, seperti sertifikasi ISO yang diisyaratkan
223.	(2) Ketentuan lebih lanjut mengenai transfer Data Pribadi sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Pemerintah.	
224.	BAB VII SANKSI ADMINISTRATIF	

225.	Pasal 50 (1) Pelanggaran terhadap ketentuan Pasal 21 ayat (1), Pasal 24, Pasal 25 ayat (1), Pasal 26 ayat (1), Pasal 27, Pasal 28, Pasal 29, Pasal 30 ayat (1), Pasal 31, Pasal 32 ayat (1), Pasal 33, Pasal 34, Pasal 35, Pasal 36, Pasal 37 ayat (1), Pasal 38 ayat (1), Pasal 39 ayat (1), Pasal 40 ayat (1) dan ayat (3), Pasal 41, Pasal 42 ayat (1), Pasal 43, Pasal 45 ayat (1), Pasal 47 ayat (2), Pasal 48 ayat (1), dan Pasal 49 ayat (1) dikenai sanksi administratif.	Pada Pasal 50 ini khususnya pada Ayat (2) mengenai pemberian sanksi administratif kepada pengendali dan pemroses data disarankan untuk ditambahkan klausa berupa huruf e yang menyatakan ***"Bahwa pemberian sanksi administratif diatas dilakukan secara berjenjang, dimulai dari pemberian teguran lisan, hingga tertulis."***
226.	(2) Sanksi administratif sebagaimana dimaksud pada ayat (1) berupa:	Sanksi administratif "ganti kerugian" memerlukan uraian lebih lanjut, khususnya terkait perbedaannya dengan denda administratif. Menyertakan proses hukum dan mekanisme banding yang jelas dan tegas. Secara terpisah, RUU harus secara jelas mendefinisikan mekanisme proses hukum yang memungkinkan organisasi untuk mengajukan banding atas keputusan dan menguraikan solusi dan hukuman tertentu. Undang-undang ini seharusnya tidak membebankan tanggung jawab yang ketat. Sebaliknya, organisasi harus dapat menunjukkan bahwa mereka telah mengambil langkah-langkah keamanan dan organisasional yang sesuai untuk melindungi data pribadi dalam situasi terkait. Misalnya, baik di bawah Peraturan Perlindungan Data Umum UE (EU General Data Protection Regulations /GDPR) (Pasal 83) dan Undang-Undang Perlindungan Data Pribadi Singapura 2012 (the Singapore Personal Data Protection Act 2012; Bagian 29), hukuman yang dijatuhkan "tergantung pada situasi setiap kasus individu". GDPR misalnya, mempertimbangkan "situasi, gravitasi dan durasi pelanggaran", apakah pelanggaran tersebut disebabkan oleh "kesengajaan atau kelalaian" data

		controller atau processor, dan apakah suatu tindakan telah diambil untuk mengurangi kerugian yang diderita oleh subyek data di antara faktor-faktor lain.
227.	a. peringatan tertulis;	
228.	b. penghentian sementara kegiatan pemrosesan Data Pribadi;	
229.	c. penghapusan atau pemusnahan Data Pribadi;	
230.	d. ganti kerugian; dan/atau	
231.	e. denda administratif.	
232.	(3) Penjatuhan sanksi administratif sebagaimana dimaksud pada ayat (2) diberikan oleh Menteri.	
233.	(4) Ketentuan mengenai tata cara pengenaan sanksi administratif sebagaimana dimaksud pada ayat (3) diatur dalam Peraturan Pemerintah.	
234.	BAB VIII LARANGAN DALAM PENGGUNAAN DATA PRIBADI	
235.	Pasal 51 (1) Setiap Orang dilarang memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi.	Usulan untuk menghapus pasal 51. untuk memastikan bahwa karyawan tidak dapat secara individual bertanggung jawab atas pelanggaran badan perusahaan Undang-Undang ini harus secara jelas berlaku untuk organisasi dan perusahaan, bukan individual. RUU ini telah menghapus konsep individu yang menyediakan data atas nama pihak ketiga sebagaimana versi sebelumnya; sekarang Pasal 51 secara terang-terangan melarang pemrosesan data pribadi oleh seorang individu, atas nama pihak ketiga, bahkan mungkin saat individu tersebut bertindak dalam kapasitas pribadi atau domestik. Ketika dibaca bersama dengan Pasal 61 tentang ketetapan hukuman, pasal ini memberikan hukuman yang signifikan

		dan berat (termasuk hukuman penjara),bahkan saat individu (a) bertindak dalam kapasitas pribadi atau domestik, atau (b) adalah karyawan yang bertindak atas perintah organisasi mereka. Memberikan tanggung jawab langsung kepada seorang individu dianggap tidak proporsional karena undang-undang perlindungan data dimaksudkan untuk mengatur tindakan-tindakan badan perusahaan dan organisasi, bukan karyawan atau individu dalam kapasitas pribadi mereka. Karena itu kami merekomendasikan Pasal 51 dan 61 dihapus dari RUU. Demikian pula, mengingat bahwa tanggung jawab perorangan harus dikecualikan dari undang-undang perlindungan data, hukuman pidana pada Bab XIII bukan merupakan hukuman yang proporsional atas pelanggaran undang-undang perlindungan data karena hukuman-hukuman tersebut ditujukan kepada karyawan perseorangan. Oleh karena itu, hukuman pidana sudah seharusnya tidak dimasukkan dalam kerangka kerja privasi, dan kami merekomendasikan penghapusan semua hukuman kriminal dari undang-undang.
236.	(2) Setiap Orang dilarang secara melawan hukum mengungkapkan Data Pribadi yang bukan miliknya.	
237.	(3) Setiap Orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya.	

238.	Pasal 52 Setiap Orang dilarang secara melawan hukum memasang dan/atau mengoperasikan alat pemroses atau pengolah data visual di tempat umum atau fasilitas pelayanan publik yang dapat mengancam dan/atau melanggar pelindungan Data Pribadi.	
239.	Pasal 53 Setiap Orang dilarang secara melawan hukum menggunakan alat pemroses atau pengolah data visual yang dipasang di tempat umum dan/atau fasilitas pelayanan publik yang digunakan untuk mengidentifikasi seseorang.	
240.	Pasal 54 (1) Setiap Orang dilarang memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain atau yang dapat mengakibatkan kerugian bagi orang lain.	Mohon klarifikasi ketentuan dalam Pasal 54 terkait larangan jual beli Data Pribadi dimana jual beli Data Pribadi tidak termasuk monetisasi data pribadi. Mohon dijelaskan apakah definisi 'jual', 'beli', dan 'monetisasi' yang dimaksud disini?
241.	(2) Setiap Orang dilarang menjual atau membeli Data Pribadi.	Perlu adanya aturan yang mengatur lebih jelas mengenai penghapusan data, dan penarikan kembali data pribadi oleh pemilik data. Sebagai contoh pada Penyelenggara LPMUBTI*:* apabila pada saat pemilik data pribadi telah mengajukan aplikasi dan memberikan data pribadi untuk diproses oleh Penyelenggara, dan data telah masuk dalam tahap pemrosesan oleh Penyelenggara, maka pemilik data pribadi tidak bisa secara langsung atau serta-merta melakukan penarikan data pada saat proses tersebut secara sepihak. Karena terdapat beberapa dampak terhadap Penyelenggara dalam memberikan Layanannya, seperti: • Penyelenggara lalai dalam pembuktian rekam jejak audit kepada regulator/pengawas, sebagaimana diatur dalam peraturan perundang-undangan terkait; dan • Menghambat efektivitas dan efisiensi biaya yang telah dikeluarkan Penyelenggara

		dalam hal pelaksanaan proses data pribadi tersebut.
242.	BAB IX PEMBENTUKAN PEDOMAN PERILAKU PENGENDALI DATA PRIBADI	
243.	Pasal 55 (1) Asosiasi pelaku usaha dapat membentuk pedoman perilaku Pengendali Data Pribadi.	Penyusunan Pedoman Perilaku Pengendali Data Pribadi/Standar Industri di RUU PDP Isu hak pemilik data dan permintaan data oleh pemerintah dalam konteks produk yang ditawarkan dengan perusahaan sector lain (contoh: PAYDI, Banccasurance, kolaborasi dengan Fintech) memerlukan: • Perlunya peran independent mediator untuk isu lintas sektoral • Penguatan peran asosiasi di RUU PDP cukup kuat sebagai SRO • Kerangka kerjasama antara asosiasi yang industrinya saling berkolaborasi Hal ini penting untuk mengatur limitation of liabilities - agar perusahaan tidak menjadi primary liability dalam implementasi PDP yang melibatkan pihak ketiga.
244.	(2) Asosiasi pelaku usaha dalam membentuk pedoman perilaku Pengendali Data Pribadi sebagaimana dimaksud pada ayat (1), harus mempertimbangkan:	
245.	a. tujuan pemrosesan Data Pribadi;	
246.	b. prinsip pelindungan Data Pribadi; dan	
247.	c. kepentingan Pemilik Data Pribadi atau asosiasi perwakilannya.	
248.	(3) Pedoman perilaku Pengendali Data Pribadi sebagaimana dimaksud pada ayat (1) harus memiliki tingkat pelindungan yang setara atau lebih tinggi dari Undang-Undang ini.	Hal ini akan kembali berdampak terhadap masalah harmonisasi mengenai perlindungan data di setiap sektor industri. Bagaimana cara untuk menentukan bahwa pemenuhan persyaratan memiliki tingkat perlindungan yang setara atau

		lebih tinggi? Siapa yang akan melakukan pemeriksaan tersebut?
249.	(4) Pedoman perilaku Pengendali Data Pribadi sebagaimana dimaksud pada ayat (3) tidak boleh bertentangan dengan Undang-Undang ini.	
250.	BAB X PENYELESAIAN SENGKETA DAN HUKUM ACARA	
251.	Pasal 56 (1) Penyelesaian sengketa pelindungan Data Pribadi dilakukan melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan.	
252.	(2) Hukum acara yang berlaku dalam penyelesaian sengketa dan/atau proses pengadilan pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan hukum acara yang berlaku sesuai dengan ketentuan perundang-undangan.	
253.	(3) Alat bukti yang sah dalam Undang-Undang ini adalah:	
254.	a. alat bukti sebagaimana dimaksud dalam hukum acara; dan	
255.	b. alat bukti lain berupa informasi elektronik dan/atau dokumen elektronik sesuai dengan peraturan perundang-undangan.	
256.	(4) Dalam hal diperlukan untuk melindungi Data Pribadi, proses persidangan dilakukan secara tertutup.	
257.	BAB XI KERJA SAMA INTERNASIONAL	
258.	Pasal 57 (1) Kerja sama internasional dilakukan oleh Pemerintah dengan pemerintah negara lain atau organisasi internasional terkait dengan pelindungan Data Pribadi.	

259.	(2) Kerja sama internasional dalam rangka pelaksanaan Undang-Undang ini dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan dan prinsip hukum internasional.	
260.	BAB XII PERAN PEMERINTAH DAN MASYARAKAT	
261.	Pasal 58 (1) Pemerintah berperan dalam mewujudkan penyelenggaraan pelindungan Data Pribadi sesuai dengan ketentuan Undang-Undang ini.	
262.	(2) Penyelenggaraan pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Menteri.	
263.	(3) Ketentuan mengenai penyelenggaraan pelindungan Data Pribadi sebagaimana dimaksud pada ayat (2) diatur dalam Peraturan Pemerintah.	
264.	Pasal 59 (1) Demi kepentingan umum dan/atau kepentingan nasional, kejaksaan selaku pengacara negara berwenang bertindak untuk dan atas nama negara atau pemerintah atas pelanggaran terhadap pelindungan Data Pribadi baik yang dilakukan di dalam negeri maupun di luar negeri.	Itulah sebabnya harus ada sanksi PIDANA. Saksi adminitratif kecenderungan Perdata.
265.	(2) Pelaksanaan kewenangan sebagaimana dimaksud pada ayat (1) dilakukan baik di dalam maupun di luar pengadilan.	
266.	Pasal 60 (1) Masyarakat dapat berperan baik secara langsung maupun tidak langsung dalam mendukung terselenggaranya pelindungan Data pribadi.	
267.	(2) Pelaksanaan peran sebagaimana dimaksud pada ayat (1) dapat dilakukan melalui pendidikan, pelatihan, advokasi, dan/atau sosialisasi.	
268.	BAB XIII KETENTUAN PIDANA	Kami menyoroti hadirnya ketentuan akan sanksi pidana di RUU PDP ini. Sebagai pelaku usaha dalam ekosistem digital di Indonesia, menurut kami perlu diadakan kajian lebih lanjut untuk menentukan formulasi pemidanaan yang tepat sehingga hadirnya ketentuan ini tidak

		menghambat perkembangan ekosistem digital di Indonesia. Kami mengusulkan menghapus hukuman pidana berdasarkan Bab XIII karena hukuman pidana badan tidak sebanding.
269.	Pasal 61 (1) Setiap Orang yang dengan sengaja memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi sebagaimana dimaksud dalam Pasal 51 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah).	Sanksi yang diatur didalam Pasal 61 RUU PDP ini, tumpang tindih dengan sanksi yang diatur didalam Pasal 95A Undang-Undang Administrasi Kependudukan dimana kedua pasal tersebut mengatur hal yang sama mengenai pelanggaran data pribadi dengan ketentuan pidana penjara paling lama 2 (dua) tahun dan pidana denda paling banyak Rp25.000.000,00 (dua puluh lima juta rupiah). Disamping itu, sanksi pidana untuk Korporat harus mengacu pada peraturan yang berlaku tentang pertanggungjawaban pidana korporasi dan tidak diatur oleh Undang-undang ini. Undang-Undang ini harus secara jelas berlaku untuk organisasi dan perusahaan, bukan individual. RUU ini telah menghapus konsep individu yang menyediakan data atas nama pihak ketiga sebagaimana versi sebelumnya; sekarang Pasal 51 secara terang-terangan melarang pemrosesan data pribadi oleh seorang individu, atas nama pihak ketiga, bahkan mungkin saat individu tersebut bertindak dalam kapasitas pribadi atau domestik. Ketika dibaca bersama dengan Pasal 61 tentang ketetapan hukuman, pasal ini memberikan hukuman yang signifikan dan berat (termasuk hukuman penjara),bahkan saat individu (a) bertindak dalam kapasitas pribadi atau domestik, atau (b) adalah karyawan yang bertindak atas perintah organisasi mereka. Memberikan tanggung jawab langsung kepada seorang individu

		dianggap tidak proporsional karena undang-undang perlindungan data dimaksudkan untuk mengatur tindakan-tindakan badan perusahaan dan organisasi, bukan karyawan atau individu dalam kapasitas pribadi mereka. Karena itu kami merekomendasikan Pasal 51 dan 61 dihapus dari RUU. Demikian pula, mengingat bahwa tanggung jawab perorangan harus dikecualikan dari undang-undang perlindungan data, hukuman pidana pada Bab XIII bukan merupakan hukuman yang proporsional atas pelanggaran undang-undang perlindungan data karena hukuman-hukuman tersebut ditujukan kepada karyawan perseorangan. Oleh karena itu, hukuman pidana sudah seharusnya tidak dimasukkan dalam kerangka kerja privasi, dan kami merekomendasikan penghapusan semua hukuman kriminal dari undang-undang. Kami usulkan untuk menghapus sanksi Pidana dari RUU
270.	(2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (2) dipidana dengan pidana penjara paling lama 2 (dua) tahun atau pidana denda paling banyak Rp20.000.000.000,00 (dua puluh miliar rupiah).	
271.	(3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (3) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak Rp70.000.000.000,00 (tujuh puluh miliar rupiah).	

272.	Pasal 62 Setiap Orang yang dengan sengaja dan melawan hukum memasang dan/atau mengoperasikan alat pemroses atau pengolah data visual di tempat umum atau fasilitas pelayanan publik yang dapat mengancam atau melanggar pelindungan Data Pribadi sebagaimana dimaksud dalam Pasal 52, dipidana dengan pidana penjara paling lama 1 (satu) tahun atau pidana denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).	
273.	Pasal 63 Setiap Orang yang dengan sengaja dan melawan hukum menggunakan alat pemroses atau pengolah data visual yang dipasang di tempat umum dan/atau fasilitas pelayanan publik yang digunakan untuk mengidentifikasi seseorang sebagaimana dimaksud dalam Pasal 53 dipidana dengan pidana penjara paling lama 1 (satu) tahun atau pidana denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).	
274.	Pasal 64 (1) Setiap Orang yang dengan sengaja memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain atau yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 54 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak Rp60.000.000.000,00 (enam puluh miliar rupiah).	
275.	(2) Setiap Orang yang dengan sengaja menjual atau membeli Data Pribadi sebagaimana dimaksud dalam Pasal 54 ayat (2) dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah).	
276.	Pasal 65 Selain dijatuhi pidana sebagaimana dimaksud dalam Pasal 61 sampai dengan Pasal 64 terhadap terdakwa juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian.	

277.	Pasal 66 (1) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 61 sampai dengan Pasal 64 dilakukan oleh Korporasi, pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau Korporasi.	
278.	(2) Pidana yang dapat dijatuhkan terhadap Korporasi hanya pidana denda.	
279.	(3) Pidana denda yang dijatuhkan kepada Korporasi paling banyak 3 (tiga) kali dari maksimal pidana denda yang diancamkan.	
280.	(4) Selain dijatuhi pidana denda sebagaimana dimaksud pada ayat (2), Korporasi dapat dijatuhi pidana tambahan berupa:	
281.	a. perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana;	
282.	b. pembekuan seluruh atau sebagian usaha Korporasi;	
283.	c. pelarangan permanen melakukan perbuatan tertentu;	
284.	d. penutupan seluruh atau sebagian tempat usaha dan/atau kegiatan Korporasi;	
285.	e. melaksanakan kewajiban yang telah dilalaikan; dan	
286.	f. pembayaran ganti kerugian.	
287.	Pasal 67 (1) Jika pengadilan menjatuhkan putusan pidana denda, terpidana diberikan jangka waktu 1 (satu) bulan sejak putusan telah memperoleh kekuatan hukum tetap untuk membayar denda tersebut.	**Menyertakan proses hukum dan mekanisme banding yang jelas dan tegas.** Secara terpisah, RUU harus secara jelas mendefinisikan mekanisme proses hukum yang memungkinkan organisasi untuk mengajukan banding atas keputusan dan menguraikan solusi dan hukuman tertentu. Undang-undang ini seharusnya tidak membebankan

		tanggung jawab yang ketat. Sebaliknya, organisasi harus dapat menunjukkan bahwa mereka telah mengambil langkah-langkah keamanan dan organisasional yang sesuai untuk melindungi data pribadi dalam situasi terkait. Misalnya, baik di bawah Peraturan Perlindungan Data Umum UE (EU General Data Protection Regulations /**GDPR**) (Pasal 83) dan Undang-Undang Perlindungan Data Pribadi Singapura 2012 (the Singapore Personal Data Protection Act 2012; Bagian 29), hukuman yang dijatuhkan "tergantung pada situasi setiap kasus individu". GDPR misalnya, mempertimbangkan "situasi, gravitasi dan durasi pelanggaran", apakah pelanggaran tersebut disebabkan oleh "kesengajaan atau kelalaian" data controller atau processor, dan apakah suatu tindakan telah diambil untuk mengurangi kerugian yang diderita oleh subyek data di antara faktor-faktor lain
288.	(2) Dalam hal terdapat alasan kuat, jangka waktu sebagaimana dimaksud pada ayat (1) dapat diperpanjang untuk waktu paling lama 1 (satu) bulan.	
289.	(3) Jika terpidana tidak membayar pidana denda dalam jangka waktu sebagaimana dimaksud pada ayat (1) atau ayat (2) maka harta kekayaan atau pendapatan terpidana dapat disita dan dilelang oleh Jaksa untuk melunasi pidana denda yang tidak dibayar.	
290.	(4) Jika penyitaan dan pelelangan harta kekayaan atau pendapatan sebagaimana dimaksud pada ayat (3) tidak cukup atau tidak memungkinkan untuk dilaksanakan, pidana denda yang tidak dibayar diganti dengan pidana penjara paling lama sebagaimana diancamkan untuk tindak pidana yang bersangkutan.	
291.	(5) Lamanya pidana penjara sebagaimana dimaksud pada ayat (4) yang ditentukan oleh hakim, dicantumkan dalam putusan pengadilan.	

292.	Pasal 68 (1) Dalam hal penyitaan dan pelelangan harta kekayaan atau pendapatan sebagaimana dimaksud dalam Pasal 67 ayat (4) dilakukan terhadap terpidana Korporasi dan tidak cukup untuk melunasi pidana denda, Korporasi dikenakan pidana pengganti berupa pembekuan sebagian atau seluruh kegiatan usaha Korporasi untuk jangka waktu paling lama 5 (lima) tahun.	
293.	(2) Lamanya pembekuan sebagian atau seluruh kegiatan usaha Korporasi sebagaimana dimaksud pada ayat (1) yang ditentukan oleh hakim, dicantumkan dalam putusan pengadilan.	
294.	Pasal 69 Ketentuan sebagaimana dimaksud dalam Pasal 67 dan Pasal 68 juga berlaku dalam hal terdakwa dijatuhi pidana tambahan berupa pembayaran ganti kerugian.	
295.	BAB XIV KETENTUAN PERALIHAN	
296.	Pasal 70 Pada saat Undang-Undang ini mulai berlaku, pihak yang telah melakukan pemrosesan Data Pribadi, wajib menyesuaikan dengan ketentuan pemrosesan Data Pribadi berdasarkan Undang-Undang ini paling lama 2 (dua) tahun sejak Undang-Undang ini diundangkan.	Kami sangat menyarankan agar para pihak diizinkan setidaknya dua (2) tahun untuk mematuhi ketentuan-ketentuan dalam RUU ini. Kami selanjutnya merekomendasikan bahwa data pribadi yang telah dikumpulkan dan / atau diproses oleh pengontrol data dan / atau pemroses data (sesuai dan sesuai dengan peraturan yang berlaku) harus dikeluarkan dari ruang lingkup RUU dan persyaratan dalam RUU hanya akan berlaku untuk Data Pribadi baru yang dikumpulkan setelah RUU tersebut diberlakukan.
297.	BAB XV KETENTUAN PENUTUP	
298.	Pasal 71 Pada saat Undang-Undang ini mulai berlaku, semua ketentuan peraturan perundang-undangan yang mengatur mengenai pelindungan Data Pribadi dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam Undang-Undang ini.	

299.	Pasal 72 Undang-Undang ini mulai berlaku pada tanggal diundangkan.	
300.	Agar setiap orang mengetahuinya, memerintahkan pengundangan Undang-Undang ini dengan penempatannya dalam Lembaran Negara Republik Indonesia.	Jika pengendali data telah melakukan atau menerapkan UU PDP sesuai dengan ketentuan yang berlaku, bagaimana perlindungannya bagi pengendali data jika terjadi kebocoran data yang disebabkan oleh pihak lain tidak bertanggung jawab?
301.	Disahkan di Jakarta pada tanggal … PRESIDEN REPUBLIK INDONESIA, JOKO WIDODO	
302.	Diundangkan di Jakarta pada tanggal … MENTERI HUKUM DAN HAK ASASI MANUSIA REPUBLIK INDONESIA, YASONNA H. LAOLY	
303.	LEMBARAN NEGARA REPUBLIK INDONESIA TAHUN … NOMOR …	

IV. Masukan atas Penjelasan Rancangan Undang-Undang Pelindungan Data Pribadi Bagian Penjelasan

Berikut ini adalah masukan Asosiasi Fintech Indonesia (AFTECH) atas Penjelasan Rancangan Undang-Undang Pelindungan Data Pribadi:

NO.	RUU TENTANG PELINDUNGAN DATA PRIBADI	MASUKAN

1.	RANCANGAN PENJELASAN ATAS UNDANG-UNDANG REPUBLIK INDONESIA NOMOR … TAHUN … TENTANG PELINDUNGAN DATA PRIBADI	
2.	I. UMUM	
3.	Perkembangan teknologi informasi dan komunikasi yang melaju dengan pesat telah menimbulkan berbagai peluang dan tantangan. Teknologi informasi memungkinkan manusia untuk saling terhubung tanpa mengenal batas-batas wilayah negara sehingga merupakan salah satu faktor pendorong globalisasi. Berbagai sektor kehidupan telah memanfaatkan sistem teknologi informasi, seperti penyelenggaraan *electronic commerce* (*e-commerce*) dalam sektor perdagangan/bisnis, *electronic education* (*e-education*) dalam bidang pendidikan, *electronic health* (*e-health*) dalam bidang kesehatan, *electronic government* (*e-government*) dalam bidang pemerintahan, serta teknologi informasi yang dimanfaatkan dalam bidang lainnya. Pemanfaatan teknologi informasi tersebut mengakibatkan Data Pribadi seseorang sangat mudah untuk dikumpulkan dan dipindahkan dari satu pihak ke pihak lain tanpa sepengetahuan Pemilik Data Pribadi, sehingga mengancam hak atas privasi seseorang.	
4.	Pelindungan atas Data Pribadi adalah termasuk ke dalam pelindungan hak asasi manusia, dengan demikian, pengaturan menyangkut hak privasi atas data pribadi merupakan manifestasi pengakuan dan pelindungan atas hak-hak dasar manusia. Keberadaan suatu Undang-Undang tentang Pelindungan atas Data Pribadi merupakan suatu keharusan yang tidak dapat ditunda-tunda lagi karena sangat mendesak bagi berbagai kepentingan nasional. Pergaulan internasional Indonesia turut menuntut adanya pelindungan atas Data Pribadi. Pelindungan tersebut dapat memperlancar perdagangan, industri, investasi yang bersifat transnasional.	
5.	Undang-Undang tentang Pelindungan Data Pribadi merupakan amanat dari Pasal 28G ayat	

	(1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa, “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.” Persoalan pelindungan terhadap Data Pribadi muncul karena keprihatinan akan pelanggaran terhadap Data Pribadi yang dapat dialami oleh orang dan/atau badan hukum. Pelanggaran tersebut dapat menimbulkan kerugian yang tidak hanya bersifat materiil tetapi juga moril.	
6.	Perumusan aturan tentang pelindungan Data Pribadi dapat dipahami karena adanya kebutuhan untuk melindungi hak-hak individual di dalam masyarakat sehubungan dengan pemrosesan Data Pribadi baik yang dilakukan secara elektronik atau manual menggunakan perangkat olah data. Pelindungan yang memadai atas Data Pribadi akan mampu memberikan kepercayaan masyarakat untuk menyediakan Data Pribadi guna berbagai kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak-hak pribadinya. Dengan demikian, pengaturan ini akan menciptakan keseimbangan antara hak-hak individu dan masyarakat yang diwakili kepentingannya oleh negara. Pengaturan tentang pelindungan Data Pribadi ini akan memberikan kontribusi yang besar terhadap terciptanya ketertiban dan kemajuan dalam masyarakat informasi.	
7.	Untuk mengurangi tumpang tindih ketentuan tentang pelindungan Data Pribadi maka pada dasarnya ketentuan dalam Undang-Undang ini adalah standar pelindungan Data Pribadi secara umum, baik yang diproses sebagian atau keseluruhan dengan cara elektronik dan manual, dimana masing-masing sektor dapat menerapkan pelindungan Data Pribadi sesuai karakteristik sektor yang bersangkutan, mencakup ketentuan Data Pribadi yang telah diatur dalam ketentuan-ketentuan profesi.	

8.	Dasar dari perumusan norma dan pelaksanaan dalam perlindungan Data Pribadi yakni berdasarkan asas pelindungan, asas kepastian hukum, asas kepentingan umum, asas kemanfaatan, asas kehati-hatian, asas keseimbangan, dan asas pertanggungjawaban. Asas pelindungan dimaksudkan untuk memberi pelindungan kepada Pemilik Data Pribadi mengenai Data Pribadinya dan hak-hak atas Data Pribadi tersebut agar tidak disalahgunakan. Asas kepastian hukum dimaksudkan sebagai landasan hukum bagi pelindungan Data Pribadi serta segala sesuatu yang mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan. Asas kepentingan umum adalah bahwa dalam menegakkan pelindungan Data Pribadi harus memperhatikan kepentingan umum atau masyarakat secara luas. Kepentingan umum tersebut antara lain kepentingan penyelenggaraan negara dan pertahanan dan keamanan nasional. Asas kemanfaatan adalah bahwa pengaturan pelindungan Data Pribadi harus bermanfaat bagi kepentingan nasional, khususnya dalam mewujudkan cita-cita kesejahteraan umum. Asas kehati-hatian dimaksudkan agar para pihak yang terkait dengan pemrosesan dan pengawasan Data Pribadi harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian. Asas keseimbangan adalah sebagai upaya pelindungan Data Pribadi untuk menyeimbangkan antara hak-hak atas Data Pribadi di satu pihak dengan hak-hak negara yang sah berdasarkan kepentingan umum. Sedangkan asas pertanggungjawaban dimaksudkan agar semua pihak yang terkait dengan pemrosesan dan pengawasan Data Pribadi untuk bertindak secara bertanggung jawab sehingga mampu menjamin keseimbangan hak dan kewajiban para pihak yang terkait termasuk Pemilik Data Pribadi.	

9.	Pengaturan pelindungan Data Pribadi bertujuan antara lain melindungi dan menjamin hak dasar warga negara terkait dengan pelindungan diri pribadi, menjamin masyarakat untuk mendapatkan pelayanan dari pemerintah, Korporasi, pelaku usaha, dan organisasi /institusi lainnya, mendorong pertumbuhan ekonomi digital dan industri teknologi informasi dan komunikasi, dan mendukung peningkatan daya saing industri dalam negeri.	
10.	II. PASAL DEMI PASAL	
11.	Pasal 1 Cukup jelas.	
12.	Pasal 2 Cukup jelas.	
13.	Pasal 3	
14.	Ayat (1) Cukup jelas.	Perlu adanya penjelasan terkait definisi, kriteria dan perlakuan terhadap data pribadi bersifat umum dan khusus
15.	Ayat (2)	
16.	Huruf a Cukup jelas.	
17.	Huruf b Cukup jelas.	
18.	Huruf c Cukup jelas.	
19.	Huruf d Cukup jelas.	
20.	Huruf e Yang dimaksud dengan Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang antara lain nomor telepon seluler.	
21.	Ayat (3)	
22.	Huruf a Yang dimaksud dengan “data dan	

	informasi kesehatan" yaitu catatan atau keterangan individu yang berkaitan dengan: 1) kesehatan fisik; 2) kesehatan mental; dan/atau 3) pelayanan kesehatan.	
23.	Huruf b Yang dimaksud dengan "data biometrik" yaitu data yang berkaitan dengan fisik, fisiologis, atau karakteristik perilaku individu yang memungkinkan identifikasi unik terhadap individu, seperti gambar wajah atau data daktiloskopi. Data biometrik juga menjelaskan pada sifat keunikan dan/atau karakteristik seseorang yang harus dijaga dan dirawat, termasuk namun tidak terbatas pada: 1) rekam sidik jari; 2) retina mata; dan 3) sampel DNA.	
24.	Huruf c Yang dimaksud dengan "data genetika" yaitu semua data jenis apapun mengenai karakteristik suatu individu yang diwariskan atau diperoleh selama perkembangan prenatal awal.	
25.	Huruf d Cukup jelas.	
26.	Huruf e Cukup jelas.	
27.	Huruf f Cukup jelas.	
28.	Huruf g Cukup jelas.	
29.	Huruf h Yang dimaksud dengan "data keuangan pribadi" yaitu termasuk namun tidak terbatas kepada data jumlah simpanan pada bank termasuk: 1) tabungan; 2) deposito; dan 3) data kartu kredit.	

30.	Huruf i Cukup jelas.	
31.	Pasal 4 Cukup jelas.	
32.	Pasal 5 Cukup jelas.	
33.	Pasal 6 Cukup jelas.	
34.	Pasal 7 Cukup jelas.	
35.	Pasal 8 Cukup jelas.	
36.	Pasal 9 Cukup jelas.	
37.	Pasal 10 Yang dimaksud dengan “profil seseorang” adalah termasuk tetapi tidak terbatas pada riwayat pekerjaan, kondisi ekonomi, kesehatan, preferensi pribadi, minat, keandalan, perilaku, lokasi atau pergerakan Pemilik Data Pribadi secara elektronik.	
38.	Pasal 11 Yang dimaksud dengan “mekanisme pseudonim” adalah pemrosesan Data Pribadi sedemikian rupa sehingga Data Pribadi tidak dapat dikaitkan lagi dengan Pemilik Data Pribadi tanpa menggunakan Informasi tambahan yang diberikan untuk memastikan bahwa Data Pribadi tidak dapat dikaitkan dengan Pemilik Data Pribadi yang teridentifikasi atau dapat diidentifikasi.	
39.	Pasal 12 Cukup jelas.	
40.	Pasal 13 Cukup jelas.	
41.	Pasal 14 Cukup jelas.	

42.	Pasal 15 Yang dimaksud dengan “permintaan tertulis” adalah permohonan tercatat yang disampaikan baik secara elektronik maupun nonelektronik.	
43.	Pasal 16	
44.	Ayat (1)	
45.	Huruf a Cukup jelas.	
46.	Huruf b Cukup jelas.	
47.	Huruf c Yang dimaksud dengan “kepentingan umum dalam rangka penyelenggaraan negara” antara lain penyelenggaraan administrasi kependudukan, jaminan sosial, perpajakan, kepabeanan, dan pelayanan perizinan berusaha terintegrasi secara elektronik.	
48.	Huruf d Yang dimaksud dengan “sektor jasa keuangan” adalah perbankan, pasar modal, asuransi, lembaga pembiayaan, dana pensiun, dan industri keuangan lainnya yang berada dalam pengawasan Bank Indonesia, Otoritas Jasa Keuangan, dan Lembaga Penjamin Simpanan.	Tambahkan Peer-to-Peer Lending
49.	Huruf e Yang dimaksud dengan “agregat data” adalah sekumpulan data yang terkait dengan pribadi seseorang yang tidak dapat dan/atau tidak ditujukan untuk mengidentifikasi seseorang baik langsung maupun tidak langsung.	
50.	Ayat (2) Cukup jelas.	
51.	Pasal 17	
52.	Ayat (1)	

53.	Huruf a Cukup jelas.	
54.	Huruf b Cukup jelas.	
55.	Huruf c Cukup jelas.	
56.	Huruf d Cukup jelas.	
57.	Huruf e Yang dimaksud dengan “transfer” adalah perpindahan, pengiriman, dan/atau penggandaan Data Pribadi baik secara manual maupun elektronik dari Pengendali Data Pribadi kepada pihak lain.	
58.	Huruf f Cukup jelas.	
59.	Ayat (2) Cukup jelas.	
60.	Ayat (3) Cukup jelas.	
61.	Pasal 18	
62.	Ayat (1) Yang dimaksud dengan “persetujuan yang sah” adalah persetujuan yang disampaikan secara eksplisit, tidak boleh tersembunyi atau atas dasar kekhilafan, kelalaian, atau paksaan.	Apa perbedaan persetujuan eksplisit yang diatur pada Pasal 20? Apa yang dimaksud dengan tidak boleh tersembunyi? Diusulkan untuk tambahkan bisa dalam bentuk persetujuan elektronik
63.	Ayat (2)	
64.	Huruf a Cukup jelas.	
65.	Huruf b Cukup jelas.	
66.	Huruf c Yang dimaksud “kepentingan yang sah	

	(*vital interest*) Pemilik Data Pribadi" adalah kebutuhan/keperluan untuk melindungi hal yang sangat penting bagi Pemilik Data Pribadi misalnya tentang keberadaan seseorang.	
67.	Huruf d Cukup jelas.	
68.	Huruf e Cukup jelas.	
69.	Huruf f Cukup jelas.	
70.	Pasal 19 Cukup jelas.	
71.	Pasal 20 Cukup jelas.	
72.	Pasal 21	
73.	Ayat (1) Cukup jelas.	
74.	Ayat (2)	
75.	Huruf a Cukup jelas.	
76.	Huruf b Cukup jelas.	
77.	Huruf c Cukup jelas.	
78.	Huruf d Yang dimaksud dengan "untuk kepentingan proses penegakan hukum" ialah yang dilakukan oleh hakim, jaksa/penuntut umum dan/atau penyidik yang permintaan dan/atau kebijakannya dilakukan oleh atasan yang bersangkutan sesuai dengan ketentuan peraturan perundang-undangan.	
79.	Ayat (3) Cukup jelas.	

80.	Pasal 22	
81.	Ayat (1) Yang dimaksud dengan “alat pemroses atau pengolah data visual” adalah perangkat kamera video yang digunakan untuk merekam atau mengamati orang perseorangan pada suatu ruang atau tempat tertentu mencakup *Closed Circuit Television* (CCTV) dan/atau semua alat *surveillance and monitoring* yang terus berkembang sesuai perkembangan teknologi yang akuntabilitas dan keakuratannya terjaga. Yang dimaksud dengan “tempat umum” adalah sarana yang diselenggarakan oleh Pemerintah, swasta atau perorangan yang digunakan untuk kegiatan bagi masyarakat.	Apakah ketentuan “yang digunakan untuk kegiatan bagi masyarakat” ini termasuk untuk hal-hal seperti restoran, toko retail, dsb?
82.	Ayat (2) Cukup jelas.	
83.	Pasal 23	
84.	Huruf a Cukup jelas.	
85.	Huruf b Cukup jelas.	
86.	Huruf c Yang dimaksud dengan “organisasi/institusi” termasuk organisasi internasional.	
87.	Pasal 24	
88.	Ayat (1)	
89.	Huruf a Cukup jelas.	
90.	Huruf b Cukup jelas.	
91.	Huruf c Cukup jelas.	
92.	Huruf d Cukup jelas.	

93.	Huruf e Cukup jelas.	
94.	Huruf f Jangka waktu pemrosesan Data Pribadi berlaku sepanjang masih ada kepentingan hukum yang sah.	
95.	Huruf g Cukup jelas.	
96.	Ayat (2) Kewajiban untuk menunjukan persetujuan yang telah diberikan oleh Pemilik Data Pribadi dilakukan dalam hal pemenuhan syarat sah pemrosesan Data Pribadi.	
97.	Ayat (3) Cukup jelas.	
98.	Pasal 25	
99.	Ayat (1) Cukup jelas.	
100.	Ayat (2) Penarikan kembali persetujuan pemrosesan Data Pribadi memuat antara lain alasan penarikan dan disertai bukti.	Bukti apa yang dimaksud di sini perlu diperjelas
101.	Pasal 26	
102.	Ayat (1) Permintaan penundaan dan pembatasan pemrosesan Data Pribadi yang diajukan oleh Pemilik Data Pribadi memuat antara lain alasan penundaan dan pembatasan pemrosesan Data Pribadi dan disertai bukti.	
103.	Ayat (2) Cukup jelas.	
104.	Pasal 27 Cukup jelas.	
105.	Pasal 28 Cukup jelas.	
106.	Pasal 29 Cukup jelas.	

107.	Pasal 30 Cukup jelas.	
108.	Pasal 31 Cukup jelas.	
109.	Pasal 32 Cukup jelas.	
110.	Pasal 33	
111.	Huruf a Yang dimaksud dengan “membahayakan keamanan atau kesehatan fisik atau kesehatan mental Pemilik Data Pribadi dan/atau orang lain” antara lain perubahan data riwayat penyakit yang berpotensi membahayakan keamanan diri sendiri dan/atau orang lain.	
112.	Huruf b Yang dimaksud dengan “berdampak pada pengungkapan Data Pribadi milik orang lain” antara lain perubahan Data Pribadi nasabah yang berdampak pada pengungkapan Data Pribadi orang lain.	
113.	Huruf c Cukup jelas.	
114.	Pasal 34 Cukup jelas.	
115.	Pasal 35 Cukup jelas.	
116.	Pasal 36 Cukup jelas.	
117.	Pasal 37 Cukup jelas.	
118.	Pasal 38 Cukup jelas.	
119.	Pasal 39	

120.	Ayat (1) Yang dimaksud dengan “memusnahkan Data Pribadi” adalah memusnahkan Data Pribadi hingga Data Pribadi seseorang tidak dapat lagi diidentifikasi.	Sampai sejauh apa yang dimaksud dengan “tidak dapat diidentifikasi kembali”? karena dengan menggunakan teknik digital forensik, apa pun yang sudah terekam secara elektronik masih dapat ditampilkan kembali, kecuali media penyimpanan elektronik tersebut dirusak
121.	Ayat (2) Cukup jelas.	
122.	Pasal 40	
123.	Ayat (1) Cukup jelas.	
124.	Ayat (2) Cukup jelas.	
125.	Ayat (3) Yang dimaksud dengan “dalam hal tertentu” antara lain jika kegagalan pelindungan Data Pribadi mengganggu pelayanan publik dan/atau berdampak serius terhadap kepentingan masyarakat.	Apa indikator dari mengganggu pelayanan publik? Siapa yang menentukan apakah suatu kegagalan berdampak serius terhadap kepentingan masyarakat?
126.	Pasal 41 Cukup jelas.	
127.	Pasal 42 Cukup jelas.	
128.	Pasal 43	
129.	Ayat (1) Cukup jelas.	
130.	Ayat (2) Cukup jelas.	
131.	Ayat (3) Cukup jelas.	
132.	Ayat (4) Pada saat Prosesor Data Pribadi bertindak diluar instruksi atau perintah dan tujuan yang ditetapkan Pengendali Data Pribadi maka	

	pada saat itu Prosesor Data Pribadi telah beralih menjadi Pengendali Data Pribadi untuk tujuan lain sehingga menjadi tanggung jawab pihak yang bersangkutan.	
133.	Pasal 44 Cukup jelas.	
134.	Pasal 45	
135.	Ayat (1) Yang dimaksud dengan “pejabat atau petugas yang melaksanakan fungsi pelindungan Data Pribadi” adalah pejabat atau petugas yang bertanggung jawab untuk memastikan pemenuhan kepatuhan atas prinsip pelindungan Data Pribadi dan mitigasi risiko pelanggaran pelindungan Data Pribadi.	
136.	Ayat (2) Cukup jelas.	
137.	Ayat (3) Cukup jelas.	
138.	Ayat (4) Cukup jelas.	
139.	Pasal 46 Cukup jelas.	
140.	Pasal 47 Cukup jelas.	
141.	Pasal 48	
142.	Ayat (1) Yang dimaksud dengan pemberitahuan adalah pemberitahuan kepada pemilik data pribadi atau pemberitahuan secara umum melalui media massa baik elektronik maupun nonelektronik.	
143.	Ayat (2) Cukup jelas.	
144.	Ayat (3) Cukup jelas.	

145.	Ayat (4) Yang dimaksud dengan pemberitahuan adalah pemberitahuan kepada pemilik data pribadi atau pemberitahuan secara umum melalui media massa baik elektronik maupun nonelektronik.	
146.	Pasal 49 Cukup jelas.	
147.	Pasal 50 Cukup jelas.	
148.	Pasal 51 Cukup jelas.	
149.	Pasal 52 Cukup jelas.	
150.	Pasal 53 Cukup jelas.	
151.	Pasal 54	
152.	Ayat (1) Cukup jelas.	
153.	Ayat (2) Yang dimaksud menjual atau membeli Data Pribadi tidak termasuk monetisasi Data Pribadi.	Apakah perbedaannya?
154.	Pasal 55 Cukup jelas.	
155.	Pasal 56 Cukup jelas.	
156.	Pasal 57 Cukup jelas.	
157.	Pasal 58 Cukup jelas.	
158.	Pasal 59 Cukup jelas.	
159.	Pasal 60 Cukup jelas.	

160.	Pasal 61 Cukup jelas.	
161.	Pasal 62 Cukup jelas.	
162.	Pasal 63 Cukup jelas.	
163.	Pasal 64 Cukup jelas.	
164.	Pasal 65 Cukup jelas.	
165.	Pasal 66 Cukup jelas.	
166.	Pasal 67 Cukup jelas.	
167.	Pasal 68 Cukup jelas.	
168.	Pasal 69 Cukup jelas.	
169.	Pasal 70 Cukup jelas.	
170.	Pasal 71 Cukup jelas.	
171.	Pasal 72 Cukup jelas.	
172.	TAMBAHAN LEMBARAN NEGARA REPUBLIK INDONESIA NOMOR …	