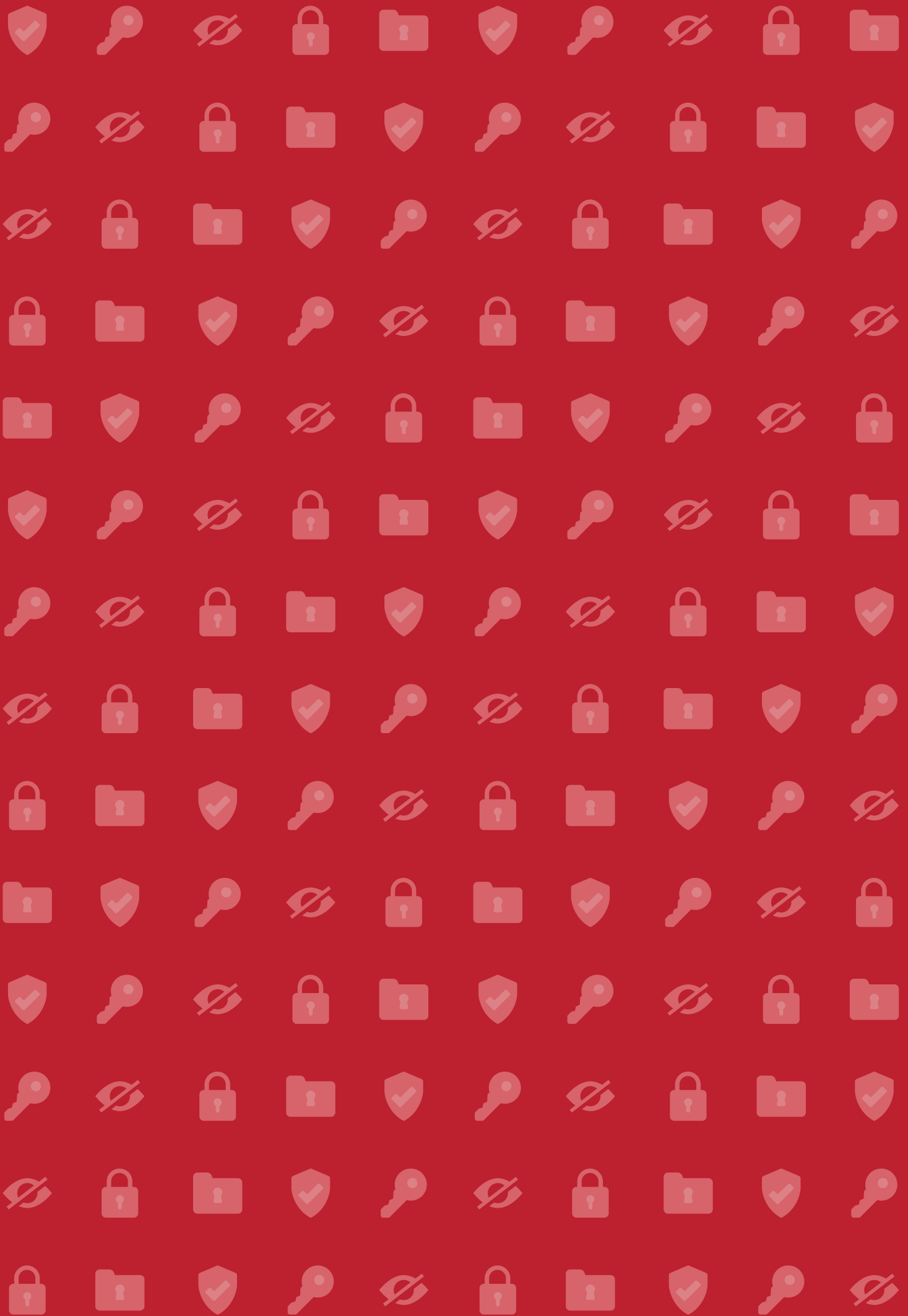


Makalah Kebijakan No. 50

Pengaturan Bersama dalam Perlindungan Data Pribadi:

**Potensi Peran Asosiasi Industri sebagai
Organisasi Regulator Mandiri**

oleh Ajisatria Suleiman, Pingkan Audrine, & Thomas Dewaranu



Makalah Kebijakan No. 50
Pengaturan Bersama dalam Perlindungan Data Pribadi:
Potensi Peran Asosiasi Industri sebagai Organisasi Regulator Mandiri

Penulis:

Ajisatria Suleiman, Pingkan Audrine, & Thomas Dewaranu
(Center for Indonesian Policy Studies)

Jakarta, Indonesia
Juli, 2022

Hak Cipta © 2022 oleh Center for Indonesian Policy Studies

Ucapan Terima Kasih:



Kami ingin mengucapkan terima kasih kepada Center for International Private Enterprise atas dukungannya dalam publikasi makalah kebijakan ini.

Penulis ingin mengucapkan terima kasih kepada Felippa Amanta atas bantuan dan masukannya selama proses penulisan makalah ini.

Sampul:

tete_escape/Freepik.com

DAFTAR ISI

Daftar Isi	5
Daftar Tabel	6
Daftar Gambar	6
Glosarium	7
Ringkasan Eksekutif	9
Pendahuluan	10
Menjelaskan Kesenjangan Regulasi: Mengapa Pengaturan Bersama dalam Perlindungan Data Pribadi Itu Penting	13
Asosiasi Industri dan Praktik-Praktik yang Digunakan Saat Ini dalam Pengaturan Bersama	20
Sejarah Pengaturan Bersama di Indonesia:	
Sektor Ekonomi & Keuangan Digital	20
Asosiasi Industri dan Perlindungan Data Pribadi:	
Praktik yang Berkembang di Sektor Keuangan Digital	23
Kode Etik AFTECH terkait Perlindungan Data Pribadi	24
Pedoman Perilaku AFPI untuk Penyelenggara Teknologi Finansial di Sektor Jasa Keuangan yang Bertanggung Jawab	26
Pelaksanaan Kode Etik AFTECH terkait Perlindungan Data Pribadi dan Pedoman Perilaku AFPI	27
Langkah Selanjutnya: Potensi Peran Asosiasi Petugas Perlindungan Data (DPO) dalam Pengaturan Bersama	30
Petugas Perlindungan Data (DPO) dalam RUU PDP dan Peraturan-Peraturan Lainnya	30
Peran dan Akuntabilitas DPO	31
Pelatihan dan Sertifikasi DPO	32
Model-model sertifikasi profesi	32
Keanggotaan Asosiasi dan Peran Etik	34
Perbandingan dengan GDPR	36
DPO di Spanyol: Peran Sentral Lembaga Perlindungan Data	37
Kesimpulan dan Rekomendasi Kebijakan	38
Referensi	40

DAFTAR TABEL

Tabel 1. Usulan Sanksi Denda atas Pelanggaran PDP	17
Tabel 2. Peraturan Sektoral yang Memberi Wewenang kepada Asosiasi.....	22
Tabel 3. Komponen-Komponen Kode Etik AFTECH terkait Perlindungan Data Pribadi.....	25
Tabel 4. Daftar Asosiasi yang Berhubungan dengan Ekosistem Ekonomi Digital dan Petugas Perlindungan Data di Indonesia.....	38

DAFTAR GAMBAR

Gambar 1. Struktur Perlindungan Data Pribadi Kemenkominfo.....	14
Gambar 2. Alur Tindakan Kemenkominfo dalam Menangani Kasus/Dugaan Pelanggaran Data Pribadi.....	15
Gambar 3. Kasus atau Insiden terkait PDP yang Ditangani oleh Kemenkominfo (2019-April 2021).....	16
Gambar 4. Mekanisme Pelatihan dan Sertifikasi Kompetensi di bawah SPKN.....	33

GLOSARIUM

BEI:

Bursa Efek Indonesia

BNSP:

Badan Nasional Sertifikasi Profesi

DPO:

Data Protection Officer (Petugas Perlindungan Data)

GDPR:

General Data Protection Regulation

ISP:

Internet Service Providers (Penyedia Layanan Internet)

KAN:

Komite Akreditasi Nasional

Kemendag:

Kementerian Perdagangan

Kemenkominfo:

Kementerian Komunikasi dan Informatika

KPEI:

Kliring Penjaminan Efek Indonesia

KSEI:

Kustodian Sentral Efek Indonesia

LSP:

Lembaga Sertifikasi Profesi yang disetujui oleh BNSP

OJK:

Otoritas Jasa Keuangan

PDP:

Perlindungan Data Pribadi

PKPA:

Pendidikan Khusus Profesi Advokat

PPDP:

Dalam RUU PDP, pemerintah Indonesia menggunakan istilah Pejabat atau Petugas Pelindung Data Pribadi untuk merujuk kepada posisi DPO

PSE:

Penyelenggara Sistem Elektronik

SKKNI:

Standar Kompetensi Kerja Nasional Indonesia

SPKN:

Sistem Pelatihan Kerja Nasional diatur oleh Undang-Undang No. 13/2003 tentang Ketenagakerjaan (UU Ketenagakerjaan) jo. Peraturan Pemerintah No. 31/2006 tentang Sistem Pelatihan Kerja Nasional (PP 31/2006).

SRO:

Self-Regulatory Organization (Organisasi Regulator Mandiri)

UU ITE:

Undang-Undang No. 11/2008 tentang Informasi dan Transaksi Elektronik dan Perubahannya No. 19/2016

RINGKASAN EKSEKUTIF

Seiring dengan ekonomi digital di Indonesia yang mengalami pertumbuhan eksponensial, muncul kebutuhan akan adanya sebuah pendekatan baru untuk mengatur kegiatan dan transaksi yang dilakukan dalam ruang ini. Hal ini terutama berlaku dalam bidang perlindungan data pribadi, dimana data personal dalam jumlah yang sangat besar dikumpulkan, diproses, dan disimpan oleh berbagai entitas untuk beragam tujuan. Adalah hal yang sulit bagi para regulator untuk mengawasi seluruh kegiatan dan memastikan kepatuhan dengan praktik-praktik terbaik dalam platform digital, baik dalam sektor publik maupun swasta. Maka dari itu, pendekatan pengaturan bersama (koregulasi) menjadi salah satu solusi yang dapat diambil untuk menangani masalah tersebut.

Pendekatan pengaturan bersama dalam perlindungan data pribadi dapat melengkapi penerapan standar-standar profesional dan teknis yang spesifik berdasarkan sektor, berfokus terhadap langkah-langkah preventif, dan melibatkan aktor-aktor non-negara dalam mekanisme penerapannya. Di Indonesia, khususnya dalam jasa keuangan, asosiasi industri telah memainkan perannya sebagai "organisasi regulator mandiri (*self-regulatory organizations*)" yang melengkapi upaya pengawasan entitas-entitas yang termasuk dalam lingkup pengaturan. Baru-baru ini, terdapat preseden untuk memperluas peran asosiasi ke ranah keuangan digital, termasuk jika terjadi pelanggaran perlindungan data pribadi. Model ini dapat diadopsi untuk platform digital dalam sektor Teknologi Informasi dan Komunikasi (TIK) secara umum. Mengambil peluang dari Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yang, menurut Pasal 55-nya, dapat memperbolehkan asosiasi industri untuk menerapkan pengaturan bersama, asosiasi industri dapat menyusun standar-standar teknisnya sendiri terkait tata kelola data pribadi yang spesifik berdasarkan sektor dan memberlakukan standar-standar tersebut melalui "penegakan aturan bersama (*peer enforcement*)". Di sisi lain, pemerintah akan tetap menjalankan fungsi pengawasan guna memastikan bahwa inisiatif-inisiatif industri ini diterapkan secara adil dan selaras dengan prinsip-prinsip persaingan pasar. Salah satu cara lain untuk menerapkan pengaturan bersama adalah dengan memberdayakan profesi Petugas Perlindungan Data (*Data Protection Officer* atau DPO) yang, berdasarkan pengalaman di negara-negara lain, dapat menetapkan standar komunitas profesional untuk praktik-praktik terbaik perlindungan data pribadi.

PENDAHULUAN

Indonesia telah mengalami ledakan ekonomi sejak lahirnya ekonomi digital. Nilai total transaksi (*Gross Merchandise Value* atau GMV) dari sektor ekonomi digital Indonesia diperkirakan akan mencapai USD 146 miliar pada tahun 2025, jauh meningkat dari USD 40 miliar pada tahun 2019 (Google, Temasek, & Bain & Company, 2021). Kendati demikian, pesatnya inovasi dan pembangunan sektor ekonomi digital di Indonesia belum sepenuhnya dibarengi oleh kerangka regulasi yang sigap, dalam artian mengikuti kebutuhan. Kesigapan inilah yang diperlukan untuk mendorong pertumbuhan industri sembari menyediakan perlindungan hukum yang memadai bagi konsumen. Kurangnya kerangka regulasi yang mengikuti kebutuhan dapat dilihat dari ketiadaan undang-undang nasional tentang perlindungan data pribadi di Indonesia dan Undang-Undang (UU) Perlindungan Konsumen No. 8/1999 yang sudah ketinggalan zaman.

Penanganan data pribadi yang tidak tepat dapat berdampak negatif bagi konsumen, membuat mereka rentan terhadap risiko-risiko penipuan akibat pelanggaran data, pelanggaran hak privasi, dan potensi eksploitasi. Perlindungan data pribadi adalah hal yang esensial dalam privasi dan keamanan, sehingga membutuhkan perhatian dan aksi dari pemerintah, sektor swasta, dan masyarakat.

Perlindungan data pribadi merupakan tulang punggung yang krusial dalam ekonomi digital. Platform-platform digital komersial mengumpulkan, memproses, dan memonetisasi data pribadi dalam jumlah yang sangat besar untuk menghasilkan pendapatan melalui iklan atau cara-cara lain. Berbagai lembaga sektor publik juga mengumpulkan dan memproses data untuk aneka tujuan, mulai dari penyelenggaraan layanan publik hingga pengawasan. Penanganan data pribadi yang tidak tepat dapat berdampak negatif bagi konsumen, membuat mereka rentan terhadap risiko-risiko penipuan akibat pelanggaran data, pelanggaran hak privasi, dan potensi eksploitasi. Perlindungan data pribadi adalah hal yang esensial dalam privasi dan keamanan, sehingga membutuhkan perhatian dan aksi dari pemerintah, sektor swasta, dan masyarakat. Kerangka perlindungan data dapat membantu menumbuhkan kepercayaan konsumen dan meningkatkan adopsi digital, yang pada akhirnya mendorong investasi, kompetisi, dan inovasi dalam ekonomi digital Indonesia.

Dalam konteks ini, terdapat dua tantangan besar terkait regulasi yang hadir dalam sektor ekonomi digital: (i) kurangnya lanskap regulasi yang koheren yang mengatur ekonomi digital—khususnya mengenai perlindungan data; dan (ii) pendekatan pemerintah-sentris yang persisten dalam membuat kebijakan, yang menghambat pendekatan kolaboratif untuk menanggapi tantangan-tantangan yang ada. Perlindungan data adalah isu yang melibatkan berbagai pemangku kepentingan dalam ekonomi digital.

Terkait tantangan pertama, sebagaimana ditunjukkan oleh Aprilianti dan Dina (2021), ada setidaknya 14 kementerian dan lembaga pemerintah yang mengatur sektor ekonomi digital dengan lebih dari 60 peraturan perundang-undangan dan regulasi yang berlaku. Lebih dari setengah peraturan perundang-undangan dan regulasi tersebut berhubungan dengan perlindungan data pribadi dengan fokus yang spesifik berdasarkan sektornya, seperti telekomunikasi, informasi dan transaksi elektronik, perbankan dan keuangan, operator sistem

elektronik, administrasi pemerintahan, dan kesehatan. Akan tetapi, sejumlah peraturan saling tumpang tindih dan berlawanan antara satu sama lain. Salah satu contohnya adalah perbedaan klasifikasi data pribadi yang ada di dalam dua peraturan: UU Informasi dan Transaksi Elektronik (UU ITE) No. 19/2016 dan UU Administrasi Kependudukan No. 24/2013 (Riyadi, 2021).¹ Maka dari itu, penyusunan UU Perlindungan Data Pribadi yang mencakup seluruh sektor akan menjadi krusial sebagai dasar hukum perlindungan data dan privasi. Upaya ini perlu diikuti dengan harmonisasi tindakan pencegahan atau amandemen undang-undang yang telah ada yang berisi ketentuan-ketentuan mengenai perlindungan data yang saling berlawanan.

Pada tahun 2014, Kementerian Komunikasi dan Informatika (Kemenkominfo) mulai menggodok Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) dan menyerahkannya kepada pemerintah pada tahun 2020 (Karunian, 2020). Meski RUU ini sudah dimasukkan ke dalam Program Legislasi Nasional tahun 2020, 2021, dan 2022, pembahasannya masih belum selesai. Pandangan-pandangan yang berbeda antara Kemenkominfo dan anggota DPR seputar ketentuan-ketentuan otoritas perlindungan data pribadi menyebabkan pembahasan RUU ini mandek hingga tulisan ini dipublikasikan pada Juli 2022.

Terkait tantangan kedua, pendekatan tradisional yang dipakai dalam membuat kebijakan dan tata kelola, yang cenderung menggunakan metode komando dan kendali, yang juga dikenal sebagai pendekatan atas-bawah (*top-down*) atau dikendalikan oleh negara (*state-controlled*), bisa jadi tidak cocok dengan sektor ekonomi digital yang berkembang pesat dan sifatnya sangat teknis. Pendekatan pengaturan bersama dalam sektor ekonomi digital akan memerlukan input yang menyeluruh dan berkelanjutan dari berbagai pemangku kepentingan di dalam proses pembuatan kebijakannya, serta pembagian tanggung jawab antara pemangku kepentingan pemerintah dan non-pemerintah dalam proses implementasi dan evaluasinya, sebagaimana telah diusulkan (Finck, 2017; Torfing *et al.*, 2016; dan Hepburn, 2018).

Center for Indonesian Policy Studies (CIPS) telah melakukan sejumlah studi yang mengkaji biaya dan manfaat dari penerapan pendekatan pengaturan bersama dalam ekonomi digital Indonesia. Studi-studi tersebut menemukan bahwa ekonomi digital Indonesia akan dapat diuntungkan dan semakin berkembang jika terdapat ruang yang memungkinkan peran lebih aktif dan pemberian tugas kepada pemangku kepentingan non-pemerintah dalam mengimplementasikan kebijakan-kebijakan ekonomi digital, sehingga lebih banyak inovasi dapat dibuat dan masalah-masalah digital dapat diatasi secara efektif berdasarkan kapasitas setiap pemangku kepentingan. Misalnya, pemerintah dapat berfokus pada proses pembuatan regulasi dan pengawasannya, sedangkan peran besar lainnya dapat diambil oleh asosiasi usaha atau industri, salah satunya dengan mengedukasi pengguna melalui program-program literasi dan pengembangan kapasitas untuk para talenta digital (Aprilianti & Dina, 2021; Riyadi, 2021; Suleiman, 2021; dan Audrine & Murwani, 2021).

¹ Menurut Undang-Undang Administrasi Kependudukan No. 24/2013, data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenarannya serta dilindungi kerahasiaannya. Tidak ada kategorisasi lebih lanjut terkait data apa saja yang termasuk dalam definisi ini. Sementara itu, di dalam UU ITE, kategorisasinya cukup luas tanpa ada ketentuan spesifik mengenai data pribadi. Alih-alih, UU ITE menggunakan istilah data elektronik yang didefinisikan sebagai satu atau sekumpulan data, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*e-mail*), telegram, teleks, *teletype* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Makalah ini menilai pendekatan baru pengaturan bersama menggunakan instrumen asosiasi industri. Pentingnya asosiasi usaha dan profesi dalam ekonomi digital dicerminkan dalam sejumlah peraturan di Indonesia, mengingat kemampuannya untuk meregulasi secara mandiri di luar peraturan yang diberlakukan oleh pemerintah. Pasal 55 RUU PDP, misalnya, memperbolehkan asosiasi industri untuk membentuk pedoman perilaku bagi pengendali dan prosesor data dalam menangani data pribadi.² Pedoman tersebut harus mempertimbangkan prinsip-prinsip perlindungan data pribadi, tujuan terbatas penggunaan data pribadi, dan kepentingan pemilik data. Lebih lanjut lagi, RUU ini juga menekankan bahwa pedoman perilaku tidak boleh bertentangan dengan RUU, sembari menjamin tingkat perlindungan yang setidaknya setara dengan RUU PDP. Namun, industri, terkadang melalui asosiasi, sudah terlibat dalam perlindungan data di berbagai sektor digital dengan merujuk kepada sejumlah peraturan sektoral. Ini tampak jelas di sektor keuangan digital, dimana asosiasi industri telah bertindak sebagai organisasi regulator mandiri (*Self-Regulating Organizations* atau SRO) untuk menegakkan standar-standar teknis.

Mengingat bahwa pendekatan ini hanya ada di Indonesia, praktik-praktik pengaturan kolaboratif tersebut perlu dikaji lebih dalam dan dilihat bagaimana pendekatan ini akan sesuai dengan penyelenggaraan tata kelola data secara umum. Makalah ini khususnya akan membahas dua jenis asosiasi: asosiasi usaha dan asosiasi profesi. Menurut *Organization of Economic Cooperation and Development* (OECD), asosiasi usaha/industri adalah sebuah organisasi dimana perusahaan-perusahaan yang beroperasi di satu sektor yang sama dapat menjalankan upaya bersama dan membangun kerja sama berdasarkan kepentingan yang sama dalam industri tersebut (Hepburn, 2018). Jenis lainnya adalah asosiasi profesi, yaitu entitas hukum yang menyediakan wadah bagi individu-individu dengan keterampilan profesional dan visi yang sama untuk mengembangkan praktik-praktik profesi. Asosiasi jenis ini bertanggung jawab untuk membina, melindungi, dan mengembangkan keterampilan profesional anggota-anggotanya (Susanto, t.t.). Dalam kasus perlindungan data pribadi, peran Petugas Perlindungan Data (*Data Protection Officer* atau DPO) sebagai sebuah profesi telah membuat asosiasi DPO sebagai aktor utama dalam tata kelola perlindungan data pribadi.

² Draf RUU PDP yang digunakan dalam makalah ini adalah draf versi Januari 2020. Tersedia di <https://www.hukumonline.com/pusatdata/detail/lt561f74edf3260/ruu-pelindungan-data-pribadi-tahun-2020/document>

MENJELASKAN KESENJANGAN REGULASI: MENGAPA PENGATURAN BERSAMA DALAM PERLINDUNGAN DATA PRIBADI ITU PENTING

Perlindungan data pribadi merupakan inti dari ekonomi digital, terutama di Indonesia, dimana aspek ini masih sedang dikembangkan melalui berbagai langkah legislatif dan regulasi. Platform-platform digital di Indonesia, yang disebut juga sebagai Penyelenggara Sistem Elektronik (PSE), hadir baik di sektor publik maupun swasta, dan semakin banyak menghasilkan, mengumpulkan, dan memproses data masyarakat. Dalam beberapa tahun belakangan, terdapat sejumlah kejadian besar yang melibatkan pelanggaran data pribadi dimana peretas menyerang dan mencuri data dari basis data milik pemerintah. Dua kasus terbesar adalah kebocoran atau peretasan data yang dialami oleh Komisi Pemilihan Umum (KPU) dan Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS Kesehatan). Selain lembaga pemerintah, platform *marketplace* daring seperti Tokopedia dan Bukalapak dan platform konten buatan pengguna (*user-generated content*) seperti Facebook juga pernah menjadi korban kebocoran atau peretasan data.

Kerangka perlindungan data yang kuat tidak hanya akan memungkinkan adanya mekanisme untuk melawan peretas, penipu, dan pelaku kejahatan siber lainnya; tetapi juga memasang sistem pertanggungjawaban hukum bagi PSE untuk memastikan bahwa mereka mengambil tindakan-tindakan yang tepat, yakni untuk mengidentifikasi apakah mereka bertanggung jawab atas suatu kebocoran data atau menerapkan langkah-langkah preventif untuk mencegah pelanggaran serupa terjadi di masa mendatang. Dalam jangka panjang, kerangka perlindungan data akan membantu menumbuhkan kepercayaan konsumen dan meningkatkan penggunaan digital, yang akhirnya mendorong investasi, kompetisi, dan inovasi dalam ekonomi digital Indonesia.

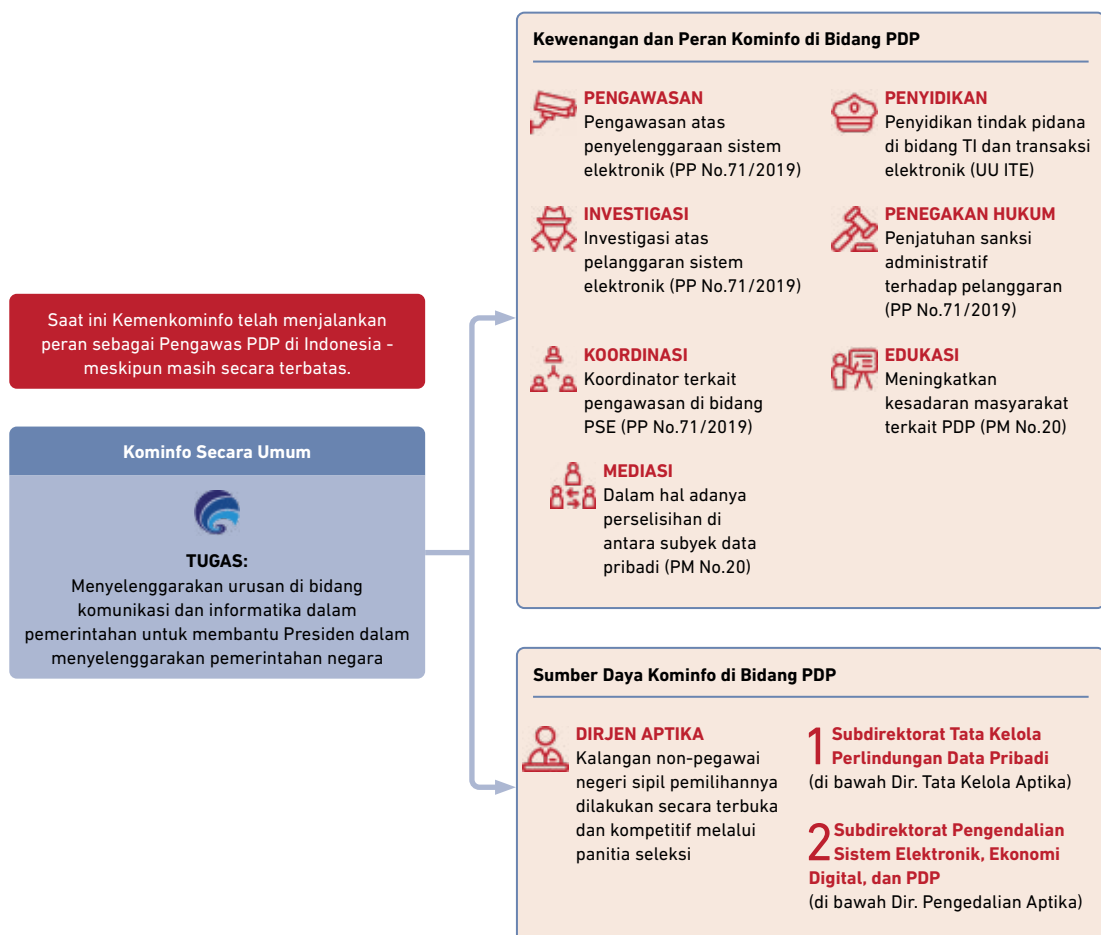
Kendati terdapat sejumlah peraturan yang berlaku di tingkat teknis, seperti PP No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019) dan di tingkat sektor jasa keuangan dan pelayanan kesehatan, sebuah peraturan di tingkat legislatif kini sedang dibahas oleh DPR, yaitu RUU PDP. Dalam kerangka regulasi ini, sektor swasta memiliki peran untuk menyusun aturan dan memastikan kepatuhannya. Sektor swasta dianggap memiliki serangkaian insentif untuk menjunjung prinsip-prinsip data pribadi demi mempertahankan kepercayaan konsumennya. Hal ini menjadi jalur yang potensial untuk mengembangkan pendekatan pengaturan bersama.

Kerangka regulasi terkait perlindungan data pribadi yang ada saat ini menggunakan pendekatan atas-bawah (*top-down*) dengan Kemenkominfo sebagai regulator and administrator utamanya. Sebagaimana diatur dalam PP No. 71/2019 dan peraturan pelaksanaannya yaitu Permenkominfo No. 5/2020, Kemenkominfo memiliki wewenang untuk mewajibkan seluruh platform—yang disebut sebagai Penyelenggara Sistem Elektronik (PSE)—untuk mendaftarkan diri ke Kemenkominfo melalui sistem *Online Single Submission* (OSS) sebelum mulai beroperasi. Kewajiban untuk

“Dalam jangka panjang, kerangka perlindungan data akan membantu menumbuhkan kepercayaan konsumen dan meningkatkan penggunaan digital, yang akhirnya mendorong investasi, kompetisi, dan inovasi dalam ekonomi digital Indonesia.”

mendaftar ini berlaku baik untuk (a) PSE dalam negeri (entitas legal Indonesia) dan (b) perusahaan PSE asing yang menyediakan layanan di wilayah Indonesia, menjalankan bisnis di Indonesia, atau menyediakan layanan yang digunakan di Indonesia. Kemenkominfo dapat menjatuhkan sanksi bagi PSE yang melanggar persyaratan dari Kemenkominfo, termasuk yang berkaitan dengan perlindungan data pribadi. Sanksi yang diberikan dapat berbentuk teguran tertulis, denda, pencabutan Tanda Daftar PSE, dan pemutusan akses yang akan memengaruhi operasional PSE yang bersangkutan di Indonesia. Sanksi yang terakhir berarti bahwa PSE tersebut tidak dapat diakses lagi di pasar Indonesia. Kemenkominfo memiliki wewenang untuk meminta Penyedia Layanan Internet (*Internet Service Providers* atau ISP) untuk memutus akses terhadap PSE yang tanda daftarnya telah dicabut.

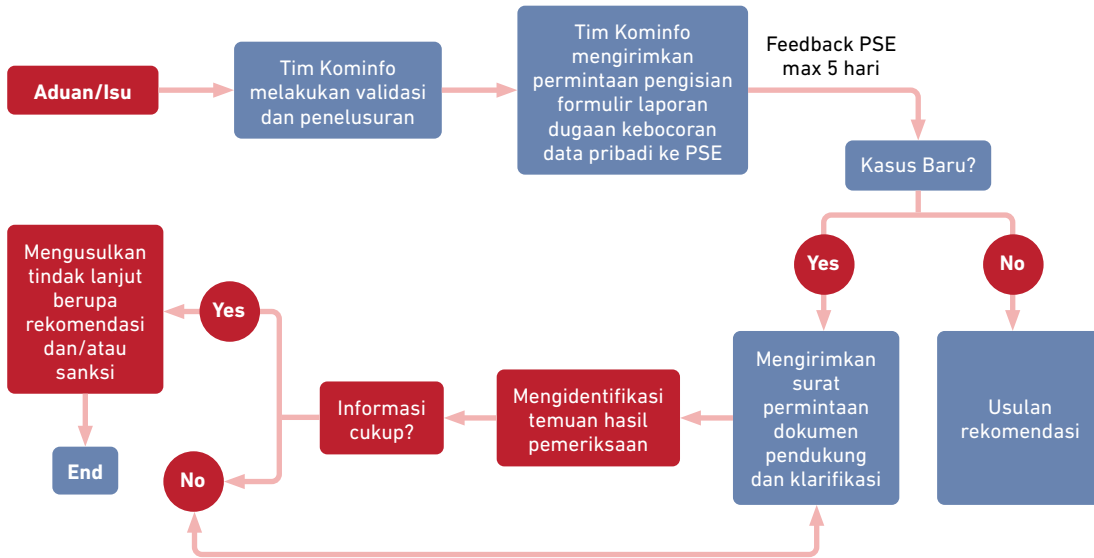
Gambar 1.
Struktur Perlindungan Data Pribadi Kemenkominfo



Sumber: Direktorat Jenderal Aplikasi Informatika Kemenkominfo (2021)

Kemenkominfo menangani keluhan-keluhan dari pengguna atau pihak ketiga mengenai dugaan kebocoran data, yang selanjutnya akan ditindaklanjuti oleh Kemenkominfo ke PSE yang bersangkutan. Selain itu, Kemenkominfo juga dapat melakukan investigasi, validasi, dan klarifikasi untuk menentukan aksi serta sanksi apabila terjadi pelanggaran atau kebocoran data.

Gambar 2.
Alur Tindakan Kemenkominfo dalam Menangani Kasus Laporan/Dugaan Kebocoran Data Pribadi



Sumber: Direktorat Jenderal Aplikasi Informatika Kemenkominfo (2021)

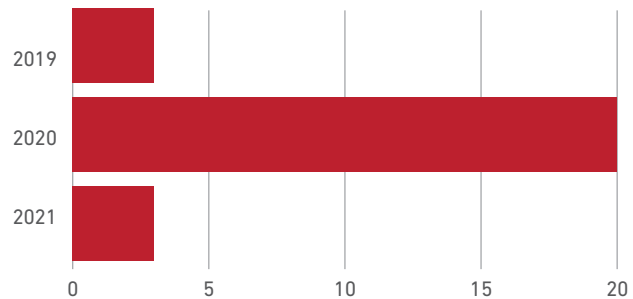
Dibekali aneka sumber daya dan sistem yang ada, Kemenkominfo telah melaksanakan mandatnya untuk mengawasi perlindungan data pribadi. Berdasarkan data Kemenkominfo, 93% dari kasus atau insiden yang mereka tangani adalah kebocoran data pribadi, dan 92% di antaranya disebabkan oleh insiden keamanan siber. Perusahaan *e-commerce* mendominasi insiden-insiden tersebut (39,3%), diikuti oleh lembaga publik (14,3%). Sejak tahun 2019 hingga 2022, Direktorat Jenderal Aplikasi Informatika mencatat terdapat 47 kasus kejahatan siber, meliputi serangan-serangan siber oleh peretas dan kebocoran data. Kemenkominfo menindaklanjuti 16 kasus untuk rekomendasi sanksi, 10 di antaranya masih dalam tahap investigasi.

Gambar 3.
Kasus atau Insiden terkait PDP yang Ditangani oleh Kemenkominfo (2019-April 2021)

Grafik kenaikan kasus pelanggaran PDP tahun 2019 - April 2021

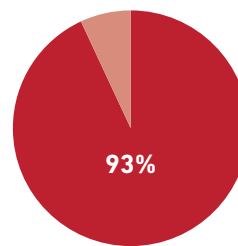
3 Kasus pada tahun 2019, 20 Kasus pada tahun 2020, dan 3 Kasus pada tahun 2021.

*Periode April 2021



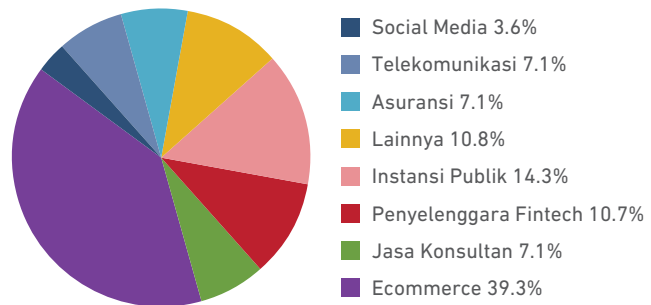
93% Kasus/Insiden yang diterima merupakan kasus kebocoran data pribadi, 7% sisanya merupakan kasus pelanggaran prinsip PDP lainnya

92% kasus kebocoran data pribadi disebabkan oleh insiden siber



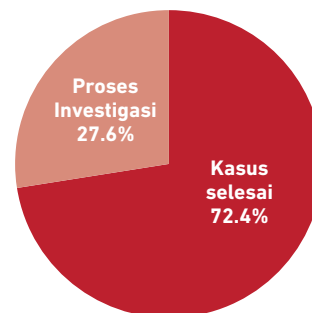
Klasifikasi PSE yang melakukan Pelanggaran Pelindungan Data Pribadi

Ecommerce merupakan penyumbang persentase terbesar untuk kasus pelanggaran Data Pribadi sepanjang tahun 2019 - Mei 2021



Penanganan Pelanggaran Pelindungan Data Pribadi

Dari 29 kasus kebocoran data pribadi sejak tahun 2019, sudah 21 kasus pelanggaran PDP telah selesai ditangani



Sumber: Direktorat Jenderal Aplikasi Informatika Kemenkominfo (2021)

Baru-baru ini, upaya Kemenkominfo untuk memperkuat wewenang pengawasannya dilengkapi dengan rencana untuk mengenakan denda dalam kasus kebocoran data pribadi. Kemenkominfo tengah menyusun draf peraturan yang berisi daftar tujuh kategori utama kebocoran atau pelanggaran data pribadi, masing-masing memiliki rinciannya sendiri-sendiri. Setiap pelanggaran memiliki poin, dimana setiap poinnya bernilai Rp 100.000 (Tabel 1). Kemenkominfo juga sedang merancang "bobot" berdasarkan ukuran PSE, dimana usaha daring mikro, kecil, menengah, dan perusahaan besar akan mendapatkan denda sebesar 25%, 50%, 75%, dan 100%, secara berturut-turut.

**Tabel 1.
Usulan Sanksi Denda atas Pelanggaran PDP**

Jenis Pelanggaran	Poin
1) Pengumpulan Data Pribadi tidak dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik Data Pribadi	
a) Tidak ada tujuan spesifik dan terbatas yang ditetapkan	1.000
b) Tidak ada landasan hukum pemrosesan data pribadi	1.000
c) Landasan hukum pemrosesan data pribadi tidak sesuai dengan peruntukannya	800
d) Tidak ada pemberitahuan mengenai informasi pemrosesan data pribadi di awal sebelum permintaan persetujuan pemilik data pribadi	50
2) Pemrosesan Data Pribadi tidak dilakukan sesuai dengan tujuannya	
a) Terdapat satu atau lebih tujuan pemrosesan data pribadi, namun data pribadi yang dikumpulkan tidak sesuai dengan tujuan yang ditetapkan tersebut	400
b) Terdapat satu atau lebih tujuan pemrosesan data pribadi, namun pemrosesan tidak sesuai dengan tujuan yang ditetapkan tersebut	700
c) Dalam hal terdapat tujuan lanjutan, tidak dilakukan analisis kesesuaian tujuan awal pengumpulan data pribadi dengan tujuan lanjutannya	200
3) Pemrosesan Data Pribadi tidak dilakukan dengan menjamin hak pemilik Data Pribadi	
4) Pemrosesan Data Pribadi tidak dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tujuan pemrosesan Data Pribadi	
a) Pemrosesan Data Pribadi dilakukan tidak akurat, lengkap, tidak menyesatkan, dan mutakhir	800
b) Pemrosesan Data Pribadi yang dilakukan tidak dapat dipertanggungjawabkan	1.000
5) Pemrosesan Data Pribadi tidak dilakukan dengan melindungi keamanan Data Pribadi dari kehilangan, penyalahgunaan, Akses, dan pengungkapan yang tidak sah, serta perubahan atau perusakan Data Pribadi	
a) Terdapat kehilangan data pribadi	10.000
b) Terdapat penyalahgunaan data pribadi	5.000
c) Terdapat akses dan pengungkapan yang tidak sah terhadap data pribadi	5.000
d) Terdapat perubahan atau perusakan data pribadi	10.000
6) Pemrosesan Data Pribadi tidak dilakukan dengan memberitahukan tujuan pengumpulan, aktivitas pemrosesan, dan kegagalan perlindungan Data Pribadi	
7) Data Pribadi tidak dimusnahkan dan/atau dihapus kecuali masih dalam masa retensi sesuai dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan	
a) Tidak memiliki kebijakan retensi	50
b) Tidak ada prosedur dan/atau kebijakan pemusnahan dan/atau penghapusan data pribadi ketika sudah tidak dalam masa retensi	150

Sumber: Direktorat Jenderal Aplikasi Informatika Kemenkominfo (2022)

Meski Kemenkominfo layak diapresiasi atas upaya menegaskan wewenangnya sebagai pengawas data pribadi melalui beragam perangkat regulasi (mulai dari pendaftaran PSE, investigasi, denda, hingga pemutusan akses), pendekatan-pendekatan yang digunakan saat ini masih belum mencakup elemen interaksi dengan sektor swasta.

Pertama, tidak ada upaya yang sistematis untuk memperbaiki kualitas sumber daya manusia dalam menghadapi isu-isu privasi dan keamanan. Yang menjadi kunci menuju praktik-praktik terbaik privasi dan keamanan adalah adanya talenta yang solid dari tenaga profesional yang akan menjaga platform dari kebocoran data atau pelanggaran atas privasi. Untuk mencapai itu, program-program pendidikan profesi dan pembelajaran eksekutif perlu diberikan secara berkelanjutan kepada tenaga profesional yang relevan. Model serupa dapat ditemukan di sektor keuangan, dimana pendidikan eksekutif untuk jenis-jenis kepakaran tertentu yang diberikan secara berkelanjutan seperti manajemen risiko menjadi suatu kewajiban.

Kedua, langkah-langkah preventif yang ada masih terbilang tidak cukup. Menurut data Kemenkominfo, 93% dari insiden yang ada merupakan akibat dari kebocoran atau pelanggaran data yang sudah terjadi. Langkah-langkah preventif membutuhkan lebih banyak upaya untuk menciptakan standar-standar teknis dan memastikan bahwa standar-standar tersebut diterapkan dengan konsisten, terlepas dari insiden privasinya.

Ketiga, seiring dengan pertumbuhan eksponensial yang dialami oleh platform akibat pesatnya peningkatan ekonomi digital, Kemenkominfo belum memiliki kapasitas dan sumber daya yang mencukupi untuk mengawasi industri secara keseluruhan. Hingga saat ini, terdapat lebih dari 4.000 PSE yang terdaftar di portal PSE milik Kemenkominfo, yang meliputi perusahaan-perusahaan Indonesia maupun asing (<https://pse.kominfo.go.id/>), dan jumlah ini diharapkan akan terus bertambah. Kemenkominfo akan membutuhkan banyak penyelidik dan pengawas dalam melaksanakan mandatnya. Pendekatan pengaturan bersama dengan mitra yang terpercaya dapat mengurangi beban sumber daya Kemenkominfo, sehingga peraturan perlindungan data pribadi dapat ditegakkan dengan serius sembari mempertahankan pendekatan regulasi internet yang mudah dan tidak membebani (*light touch*).

Keempat, karena regulator-regulator yang aktif di ruang digital berpotensi menerapkan aturan-aturannya sendiri untuk kegiatan yang sama, timbul pertanyaan mengenai siapa yang memiliki wewenang untuk menentukan apakah tindakan keamanan suatu perusahaan setara dengan tingkat perlindungan yang dijamin oleh RUU PDP—apakah itu Kemenkominfo atau otoritas pengawasan sektoral (contoh: OJK di sektor *fintech*, atau Kementerian Perdagangan di sektor *e-commerce*). Contohnya, dalam perdagangan elektronik (*e-commerce*), Pasal 58 dan 59 PP No. 80/2019 memandatkan pelaku usaha untuk mengikuti “kelaziman praktik bisnis” dalam mengelola data pribadi. Ini termasuk, antara lain, memperoleh data pribadi secara legal, mempertahankan keakuratan data dan menerapkan sistem pengamanan yang patut, serta mengumpulkan hanya data yang sesuai dengan tujuan perolehannya. Untuk kegiatan-kegiatan spesifik seperti pemasaran dan periklanan daring, Pasal 17 Permendag No. 50/2020 menekankan bahwa penggunaan data pribadi juga harus mengikuti “prinsip perlindungan konsumen dan tidak

bertentangan dengan persaingan usaha yang sehat”.³ Dengan Pasal 55 dari draf RUU PDP yang menyatakan bahwa pedoman perilaku asosiasi usaha harus “memiliki tingkat perlindungan yang setara atau lebih tinggi dari Undang-Undang ini”, asosiasi industri *e-commerce* dapat memainkan sebuah peran dalam menciptakan standar-standar teknis *e-commerce* yang menyelaraskan aturan *e-commerce* dengan peraturan perlindungan data pribadi.

³ Peraturan Pemerintah No. 80/2019 tentang Perdagangan melalui Sistem Elektronik (PP 80/2019) dan Peraturan Menteri Perdagangan No. 50/2020 (Permendag No. 50/2020) tentang Ketentuan Perizinan Usaha, Periklanan, Pembinaan, dan Pengawasan Pelaku Usaha dalam Perdagangan melalui Sistem Elektronik.

ASOSIASI INDUSTRI DAN PRAKTIK-PRAKTIK YANG DIGUNAKAN SAAT INI DALAM PENGATURAN BERSAMA

Sejarah Pengaturan Bersama di Indonesia: Sektor Ekonomi dan Keuangan Digital

Pengaturan bersama menjembatani pendekatan yang dikendalikan oleh negara (*state-controlled*) dengan pendekatan regulasi mandiri (*self-regulated*). Pengaturan bersama ditekankan pada pembagian tanggung jawab antara pemangku kepentingan negara dan non-negara. Peraturan yang dikendalikan oleh negara adalah bentuk tradisional tata kelola regulasi melalui penerbitan legislasi dan peraturan formal yang pelaksanaannya ditegakkan oleh otoritas negara. Sementara itu, aturan-aturan dalam regulasi mandiri suatu industri disusun dan dilaksanakan oleh aktor-aktor industri itu sendiri. Dengan menjembatani kedua pendekatan ini, pengaturan bersama menggabungkan pemantauan dan pelaksanaan peraturan publik dan swasta.

Dialog yang konstan dan lingkungan yang adaptif membedakan pengaturan bersama dari pendekatan-pendekatan lainnya. Penerapan dan pelaksanaan kebijakan didelegasikan oleh pemerintah secara seluruhnya atau sebagian kepada sektor swasta berdasarkan standar-standar yang telah disepakati bersama dan dialog yang berkesinambungan.

Ruang interaksi antara otoritas regulasi formal dan lembaga industri swasta (baik secara perseorangan maupun bersama di bawah asosiasi usaha) masih harus terus dikembangkan. Pengaturan bersama lebih dari sekadar intervensi yang dilakukan sekali saja untuk mendapatkan input dari pemangku kepentingan non-pemerintah ketika membuat kebijakan. Alih-alih, pengaturan bersama adalah hasil dari umpan balik yang dilakukan secara berkelanjutan, sehingga pendekatan ini menjadi sebuah proses yang eksperimental, mutual, dan adaptif (Finck, 2017; Torfing *et al.*, 2016). Dialog yang konstan dan lingkungan yang adaptif membedakan pengaturan bersama dari pendekatan-pendekatan lainnya. Penerapan dan pelaksanaan kebijakan didelegasikan oleh pemerintah secara seluruhnya atau sebagian kepada sektor swasta berdasarkan standar-standar yang telah disepakati bersama dan dialog yang berkesinambungan.

Jenis delegasi kewenangan regulasi dari otoritas pemerintah kepada sektor swasta dapat berbeda-beda tergantung dari sektornya. Sebuah lembaga industri swasta bisa menjadi bagian dari panel pemerintah yang mengonsultasikan kebijakan. Lembaga ini juga dapat diberikan wewenang untuk menerbitkan standar-standar industri untuk diadopsi sebagai aturan nasional secara formal. Pengaturan bersama dalam bentuk yang lebih luas dapat memperbolehkan lembaga swasta untuk menerbitkan peraturan dan kebijakan bagi industrinya.

Di Indonesia, lembaga swasta yang diberikan peran tertentu sebagai regulator disebut sebagai organisasi regulator mandiri (*Self-Regulatory Organization* atau SRO). SRO pertama kali diperkenalkan dalam sektor pasar modal dan sekuritas di tahun 1995, dan sejak saat itu model serupa telah dicoba untuk diperkenalkan dalam sektor digital, yang akan dibahas di bagian selanjutnya makalah ini.

Pengaturan bersama dapat menjadi opsi yang paling tepat untuk mengatasi tantangan-tantangan regulasi yang melekat pada sektor digital. Sektor digital dipenuhi dengan fragmentasi regulasi, peraturan yang tidak mengikuti perkembangan zaman, dan intervensi legislatif yang tidak tepat. Maka dari itu, karena aturan dan standar berasal dari industri itu sendiri, pengaturan bersama bisa menjadi pendekatan yang lebih relevan dan responsif terhadap kebutuhan industri.

Akan tetapi, baik regulasi mandiri maupun pengaturan bersama berisiko menyebabkan fenomena penawanan regulasi (*regulatory capture*) yang rentan terhadap perilaku anti persaingan. Misalnya, jika sektor swasta berperan dalam menetapkan standar teknis atau mengambil keputusan dalam persetujuan izin usaha perusahaan lain (misal: melalui rekomendasi industri sebagai persyaratan izin), pelaku usaha swasta yang dominan dapat menggunakan pengaruhnya untuk menerapkan standar demi keuntungannya sendiri, sehingga membatasi akses perusahaan lain untuk beroperasi dengan adil di pasar.

Seperti yang telah secara singkat disebutkan di atas, SRO pertama kali diperkenalkan pada tahun 1995 dengan diberlakukannya UU No. 8/1995 tentang Pasar Modal. SRO diberikan wewenang untuk membuat peraturan terkait kegiatan-kegiatannya, yang mengikat dan wajib diikuti oleh anggota-anggotanya. Ada tiga SRO dalam struktur pasar modal Indonesia, yaitu: Bursa Efek Indonesia (BEI), Kliring Penjaminan Efek Indonesia (KPEI), dan Kustodian Sentral Efek Indonesia (KSEI). Ketiga organisasi ini merupakan Perseroan Terbatas (PT) yang dimiliki oleh perusahaan sekuritas. Tidak ada keterlibatan negara dalam struktur kepemilikan saham BEI, KPEI, atau KSEI. BEI, contohnya, berwenang untuk mengawasi perusahaan-perusahaan sekuritas dan menjatuhkan sanksi apabila ditemukan praktik pasar yang dilarang. BEI juga bertugas meninjau dokumen perusahaan-perusahaan yang ingin menjadi perusahaan terbuka (*go public*) atau menawarkan sahamnya di bursa efek.

Konsep SRO diperkenalkan sebagai sebuah solusi untuk mengatur keuangan digital yang, serupa dengan pasar modal, memiliki kegiatan pasar yang sangat dinamis, sehingga membutuhkan tanggapan kebijakan dan pengawasan yang lebih cepat. Sejak tahun 2018, Otoritas Jasa Keuangan (OJK) Indonesia telah berupaya mendorong pembentukan SRO guna meregulasi sektor *fintech*. Asosiasi *fintech* berperan sebagai SRO yang menjadi “kepanjangan tangan OJK” dan berwenang untuk menjatuhkan sanksi atas pelanggaran yang dilakukan anggota-anggotanya. Ketua OJK, Wimboh Santoso, pada tahun 2020 memberikan pernyataan tentang pentingnya asosiasi *fintech* sebagai SRO untuk membantu OJK melaksanakan mandat pengawasannya, dikarenakan banyaknya jumlah keluhan konsumen yang diterima oleh OJK setiap hari (Setiawan, 2020).

Keputusan untuk memperbolehkan asosiasi industri *fintech* sebagai SRO menggambarkan praktik umum di sektor keuangan Indonesia yang diatur secara ketat, yang memberdayakan asosiasi industri dengan wewenang atau mandat tertentu. Model serupa dapat ditemukan di sektor-sektor lain, seperti asuransi, pembiayaan, pinjaman *fintech*, inovasi keuangan digital, dan pembayaran. Karakteristik umumnya adalah adanya pembentukan asosiasi resmi dalam peraturan sektoral dan kewajiban menjadi anggota. Pencabutan keanggotaan akan menjadi dasar untuk mencabut izin suatu usaha secara keseluruhan, membuat asosiasi seperti ini menjadi organisasi yang berkekuatan. Tabel 2 di bawah ini menyajikan contoh-contoh peraturan sektoral yang memberi wewenang kepada asosiasi.

Tabel 2.
Peraturan Sektoral yang Memberi Wewenang kepada Asosiasi

No.	Sektor	Dasar Hukum	Peran Asosiasi
1	Fintech	POJK 77/ POJK.01/2016 (<i>Peer-to-Peer Lending</i>) dan POJK 13/ POJK.01/2018 (Inovasi Keuangan Digital)	Keanggotaan wajib perusahaan pinjaman <i>fintech</i> dan inovasi keuangan digital dalam asosiasi yang telah mendapatkan persetujuan tertulis dari OJK.
2	Pembayaran	Peraturan BI No. 19/8/ PBI/2017 tentang Gerbang Pembayaran Nasional	Keanggotaan wajib perusahaan pembayaran dalam asosiasi yang telah mendapatkan persetujuan tertulis dari BI (ASPI) Asosiasi Sistem Pembayaran Indonesia (ASPI) secara resmi ditunjuk sebagai lembaga yang menetapkan standar teknis. Hingga saat ini, ASPI telah mengeluarkan standar kode QR (QRIS) dan Standar Nasional Open API (SNAP). Setelah pembahasan panjang dalam kelompok kerja ASPI, standar final secara resmi diadopsi melalui surat keputusan BI.
3	Asuransi dan Reasuransi	POJK 67 /POJK.05/2016 tentang Perizinan Usaha dan Kelembagaan Perusahaan Asuransi, Perusahaan Asuransi Syariah, Perusahaan Reasuransi, dan Perusahaan Reasuransi Syariah	Keanggotaan wajib perusahaan asuransi dan reasuransi dalam asosiasi yang telah mendapatkan persetujuan tertulis dari OJK (Pasal 70). Keanggotaan wajib tenaga ahli, aktuaris, dan auditor internal dalam asosiasi profesi. Asosiasi profesi tersebut harus mengeluarkan pernyataan bahwa calon tenaga ahli tidak sedang dalam pengenaan sanksi (Pasal 55-60). Keanggotaan wajib agen asuransi dalam asosiasi profesi. Asosiasi mendapatkan mandat eksplisit untuk melaksanakan pendaftaran agen mewakili wewenang OJK. OJK memiliki wewenang dan akses terhadap basis data agen yang dikelola oleh asosiasi (Pasal 71).
4	Pialang Asuransi dan Reasuransi	POJK 68 /POJK.05/2016 tentang Perizinan Usaha dan Kelembagaan Perusahaan Pialang Asuransi, Perusahaan Pialang Reasuransi, Perusahaan Penilai Kerugian Asuransi	Keanggotaan wajib perusahaan pialang asuransi, perusahaan pialang reasuransi, dan perusahaan penilai kerugian dalam asosiasi yang telah mendapatkan persetujuan tertulis dari OJK (Pasal 45). Keanggotaan wajib pialang asuransi dan tenaga ahli dalam asosiasi profesi. Asosiasi profesi tersebut harus mengeluarkan pernyataan bahwa calon tenaga ahli tidak sedang dalam pengenaan sanksi (Pasal 21-39).
5	Perusahaan Pembiayaan	POJK 47 /POJK.05/2020 tentang Perizinan Usaha dan Kelembagaan Perusahaan Pembiayaan dan Perusahaan Pembiayaan Syariah	Keanggotaan wajib perusahaan pembiayaan dalam asosiasi yang telah mendapatkan persetujuan tertulis dari OJK (Pasal 15 P.OJK 47 /POJK.05/2020). Keanggotaan wajib petugas keuangan, petugas penagihan, dan petugas manajemen risiko dalam asosiasi profesi. Asosiasi profesi tersebut harus mengeluarkan pernyataan bahwa calon tenaga ahli tidak sedang dalam pengenaan sanksi (Pasal 17 POJK 35 / POJK.05/2018).
6	Perantara dan Penjamin Emisi Efek Sekuritas	POJK 27/POJK.04/2014 tentang Perizinan Wakil Penjamin Emisi Efek dan Wakil Perantara Dagang Efek	Keanggotaan wajib perantara dan penjamin emisi efek dalam asosiasi profesi dan mengikuti pendidikan profesi berkelanjutan.

Sumber: Analisis penulis

Asosiasi Industri dan Perlindungan Data Pribadi: Praktik yang Berkembang di Sektor Keuangan Digital

Praktik-praktik industri yang spesifik berdasarkan sektor penting dalam menetapkan praktik perlindungan data pribadi di tingkat yang lebih teknis dan terperinci. Cara menentukan apakah dibutuhkan standar yang spesifik untuk suatu sektor adalah dengan melihat apakah sektor tersebut memiliki praktik-praktik berbeda yang membutuhkan penanganan khusus untuk melindungi data pribadi. Contohnya, di negara-negara lain, kemudahan mengumpulkan informasi biometrik atau automasi pengumpulan data dalam *Internet-of-Things* membutuhkan peraturan yang ketat tentang tujuan pengolahan informasi biometrik atau tujuan kota cerdas (*smart city*).⁴ Sementara itu, di Indonesia, sebagian besar kasus terjadi di sektor keuangan digital. Penyedia jasa keuangan tengah mengembangkan sistem *Know Your Customer* (KYC) yang terpercaya untuk meminimalkan risiko gagal bayar dengan mengumpulkan data pribadi dengan informasi identifikasi pribadi (*personally identifiable information* atau PII) tingkat tinggi. Akan tetapi, praktik ini dapat berujung pada dampak privasi yang serius ketika terjadi pelanggaran atau penyalahgunaan data.

Inilah yang menjadi alasan utama mengapa Asosiasi *Fintech* Indonesia (AFTECH), Asosiasi *Fintech* Pendanaan Bersama Indonesia (AFPI), dan Asosiasi Sistem Pembayaran Indonesia (ASPI) diberikan wewenang oleh regulator guna mengatur bersama sektor *fintech* secara aktif. Baik AFPI maupun AFTECH telah membuat pedoman perilaku mereka sendiri, yang memiliki bagian khusus tentang pengelolaan data pribadi. Pedoman perilaku ini disusun selaras dengan berbagai undang-undang, peraturan pemerintah, dan peraturan menteri tentang prinsip manajemen data yang bertanggung jawab, termasuk keamanan siber dan perlindungan data pribadi pengguna sebagaimana termaktub dalam Peraturan Pemerintah No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP No. 71/2019), Permenkominfo No. 20/2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo No. 20/2016), Peraturan Bank Indonesia 16/1/PBI/2014 tentang Perlindungan Konsumen Jasa Sistem Pembayaran, dan POJK No. 13/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan. Selain itu, banyak penyedia jasa *fintech* telah menjalani audit dan mengadopsi standar internasional seperti ISO 27001 dalam tindakan keamanan data mereka.

Kewenangan AFPI untuk ikut mengatur sektor *fintech* juga diatur lebih lanjut oleh Pasal 48 POJK No. 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi, yang mewajibkan penyelenggara layanan *fintech* untuk menjadi anggota asosiasi yang telah ditunjuk oleh OJK. Melalui surat No. S5/D.05/2019 tertanggal 17 Januari 2019, OJK menunjuk AFPI sebagai asosiasi layanan pinjam meminjam berbasis teknologi informasi yang resmi di Indonesia. Karena keanggotaan AFPI menjadi suatu kewajiban bagi penyelenggara layanan *fintech*, AFPI berwenang untuk mengembangkan instrumen regulasi mandiri, memantau kepatuhan, dan memastikan keterlaksanaannya oleh anggota-anggotanya.

⁴ Sebagai contoh, lihat standar teknis Tiongkok untuk pengenalan wajah yang melarang pengenalan wajah hanya untuk tujuan identifikasi dan tidak membuat prediksi tentang seseorang (contoh: tentang kesehatan, kinerja, atau ketertarikannya). Lihat <https://www.huntonprivacyblog.com/2021/04/29/china-publishes-draft-security-standard-on-facial-recognition/>

Kode Etik AFTECH terkait Perlindungan Data Pribadi

Peran asosiasi industri dalam perlindungan data pribadi di ekosistem ekonomi digital Indonesia diejawantahkan oleh setidaknya dua asosiasi industri besar, yaitu AFTECH dan AFPI. Terkait perlindungan data pribadi, AFTECH telah menyusun dan mengeluarkan Kode Etik Perlindungan Data Pribadi untuk diterapkan oleh anggota-anggotanya dan memastikan inovasi keuangan digital yang bertanggung jawab (AFTECH, 2021).

AFTECH berpendapat bahwa, kendati pembahasan RUU PDP sedang mengalami kemandekan, terdapat sejumlah peraturan terkait di Indonesia dan praktik-praktik terbaik yang dapat diterapkan agar layanan keuangan digital di Indonesia bisa terus berkembang secara bertanggung jawab (Wawancara 2, 2022). Maka dari itu, AFTECH membuat Kode Etik Perlindungan Data Pribadi dapat diakses oleh publik di situs webnya.

Kotak 1. Mengetahui AFTECH

Didirikan pada tahun 2016, Asosiasi Fintech Indonesia (AFTECH) telah menjadi sebuah forum bagi banyak perusahaan fintech di Indonesia untuk membahas dan berkolaborasi dengan berbagai pemangku kepentingan guna mendorong teknologi inovasi dan memperkuat daya saing industri fintech nasional.

Tiga tahun setelah didirikan, pada tanggal 9 Agustus 2019, AFTECH secara resmi ditunjuk oleh OJK sebagai asosiasi penyelenggara inovasi keuangan digital (IKD). Penunjukan ini menunjukkan perwujudan pendekatan pengaturan bersama dalam ekosistem fintech Indonesia. Saat ini, AFTECH memiliki lebih dari 350 anggota yang terdiri atas perusahaan-perusahaan startup di sektor fintech, penyedia layanan teknologi, dan jasa keuangan lainnya.

AFTECH memiliki visi "Mendorong Inklusi Keuangan melalui Layanan Keuangan Digital di Indonesia" dan misi mendukung target-target inklusi pemerintah dengan empat pilar utama, yaitu: (i) Advokasi Kebijakan; (ii) Kolaborasi Komunitas; (iii) Keaksaraan (Literasi) dan Edukasi; serta (iv) Pengembangan Pengetahuan.

Dengan dua belas kelompok kerjanya, AFTECH telah berpartisipasi dalam mendukung DPR dan pemerintah Indonesia—terutama Kementerian Komunikasi dan Informatika—dalam memberikan wawasan seputar industri fintech sebagai input dalam penyusunan RUU PDP. Praktik-praktik ilegal yang menyalahgunakan data pribadi telah menjadi keluhan publik dan konsumen, sehingga kepastian hukum terkait PDP akan meningkatkan kepercayaan masyarakat dalam layanan industri fintech.

Sumber: AFTECH (t.t.). <https://fintech.id/id/about#working-group> dan Wawancara 2 (2022)

Kode Etik terkait Perlindungan Data Pribadi dan Kerahasiaan Data di Sektor Teknologi Finansial akan selanjutnya disebut sebagai Kode Etik PDP AFTECH. Pembuatan Kode Etik ini didorong oleh kekhawatiran anggota-anggotanya tentang kepastian hukum perlindungan data pribadi bagi para konsumen sebagai pemilik data pribadi. Selain itu, Kode Etik ini juga dimaksudkan untuk meningkatkan kepercayaan masyarakat dalam menggunakan teknologi keuangan dan menunjukkan komitmen anggota-anggota AFTECH terhadap tanggung jawab kepada pemerintah dan pelaku-pelaku jasa keuangan lain dalam membuat inovasi keuangan.

Dengan mengakui wewenang pemerintah dalam membuat kebijakan, Kode Etik PDP AFTECH ini disusun berdasarkan dua peraturan utama yang mengatur tentang PDP—Permenkominfo No. 20/2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik dan Peraturan Pemerintah No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Tabel 3 di bawah ini menyajikan komponen-komponen utama Kode Etik PDP AFTECH.

Tabel 3.
Komponen-Komponen Kode Etik AFTECH terkait Perlindungan Data Pribadi

Kode Etik untuk Peraturan Industri Teknologi Keuangan		
No.	Komponen	Prinsip Utama
1	Kepatuhan terhadap Hukum, Keadilan, dan Transparansi	Memiliki dasar hukum yang jelas untuk memproses data pribadi, serta mematuhi segala ketentuan peraturan perundang-undangan yang berlaku terkait dengan data pribadi.
		Menggunakan data pribadi sesuai dengan tujuan, sewajarnya, dan tidak merugikan bagi individu yang bersangkutan.
2	Minimalisasi Data	Hanya memproses data pribadi sesuai dengan tujuan yang telah ditentukan dan disetujui oleh pemilik data pribadi.
3	Keakuratan	Data pribadi yang diproses oleh anggota AFTECH harus dijaga keakuratannya.
4	Integritas, Kerahasiaan, dan Keamanan Data	Kode Etik PDP ini tidak menyajikan secara spesifik langkah-langkah yang perlu dilakukan untuk melakukan pengamanan data pribadi yang berada di bawah kendali anggota AFTECH. Namun demikian, Kode Etik PDP ini mempercayakan kepada anggota AFTECH untuk mengambil langkah-langkah praktis dan bertanggung jawab untuk melindungi data pribadi dari pelanggaran, kehilangan, penyalahgunaan, kegagalan, atau ketidaksengajaan perubahan atau pemusnahan, sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.
5	Akuntabilitas	Semua data pribadi diproses dengan penuh tanggung jawab dan berdasar pada kepatuhan terhadap ketentuan peraturan perundang-undangan yang berlaku. Pengendalian dan pemrosesan data pribadi juga dilakukan secara proporsional sesuai dengan tujuannya, dan dengan proses yang aman dan dapat dipertanggungjawabkan.
6	Itikad Baik	Kode Etik PDP ini menekankan bahwa segala kegiatan pemrosesan data pribadi oleh anggota AFTECH dilakukan sesuai dengan persetujuan yang diperoleh dari pemilik data pribadi dan sesuai dengan ketentuan peraturan perundang-undangan yang berlaku, dan anggota AFTECH mempunyai mekanisme klarifikasi dan resolusi untuk mengatasi dugaan dan kejadian pelanggaran dan/atau kegagalan perlindungan data pribadi.
		Kode Etik PDP ini tidak mengatur secara rinci mekanisme klarifikasi dan resolusi dan mempercayakan segala mekanisme, pernyataan, dan pemberitahuan terkait pelanggaran data pribadi yang dimiliki oleh anggota AFTECH telah sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

Sumber: Diolah oleh penulis dari AFTECH. (2021). Kode Etik terkait Perlindungan Data Pribadi dan Kerahasiaan Data di Sektor Teknologi Finansial. <https://fintech.id/storage/files/shares/Kode%20Etik/Kode%20Etik%20AFTECH%20-%20TF%20PDP.pdf>

Pedoman Perilaku AFPI untuk Penyelenggara Teknologi Finansial di Sektor Jasa Keuangan yang Bertanggung Jawab

Upaya pengaturan bersama lainnya diwujudkan melalui pembuatan dan penerapan Pedoman Perilaku Bersama antara AFPI, AFTECH, dan AFSI (2019). Dibuat pada tahun 2019, Pedoman Perilaku Penyelenggara Teknologi Finansial di Sektor Jasa Keuangan yang Bertanggung Jawab ditujukan untuk menjadi pedoman bagi anggota asosiasi yang terdiri atas ratusan perusahaan *fintech* untuk menjalankan usahanya secara bertanggung jawab.

Pedoman Perilaku ini utamanya diimplementasikan berdasarkan tiga prinsip umum: (i) Transparansi Produk dan Metode Penawaran Produk Layanan; (ii) Manajemen Risiko Produk Baru; dan (iii) Penerapan Prinsip Itikad Baik.

Kotak 2. Peran AFPI

Asosiasi Fintech Pendanaan Indonesia (AFPI) dibentuk untuk menjembatani OJK dengan pelaku usaha *peer-to-peer lending* yang banyak di Indonesia. Serupa dengan AFTECH yang terlibat dalam pendekatan pengaturan bersama, OJK memberi AFPI peran yang strategis dalam menjalankan fungsi regulasi dan pengawasan berdasarkan Surat OJK No. S-D.05/IKNB/2019 dan Peraturan OJK No. 77 (POJK 77). Dengan kata lain, operator *peer-to-peer lending* diwajibkan untuk mendaftar sebagai anggota AFPI dan mematuhi pedoman perilakunya.

Dengan begitu, AFPI menjadi *gatekeeper* yang mengawasi anggota-anggotanya. AFPI juga dapat memutuskan untuk memeriksa atau meninjau ulang izin usaha perusahaan *fintech* yang melanggar Pedoman Perilaku sebelum pemerintah, atau, dalam hal ini, OJK.

Sumber: Suleiman (2021). Improving Consumer Protection for Low-Income Customers in P2P Lending. Center for Indonesian Policy Studies. <https://www.cips-indonesia.org/publications/improving-consumer-protection-for-low-income-customers-in-p2p-lending>

Pelaksanaan Kode Etik AFTECH terkait Perlindungan Data Pribadi dan Pedoman Perilaku AFPI

Dalam proses pelaksanaannya, AFTECH secara aktif bekerja sama dan berkoordinasi dengan OJK, Bank Indonesia, dan segala pemangku kepentingan yang relevan, baik dari sektor pemerintah maupun swasta, untuk meningkatkan literasi keuangan digital masyarakat Indonesia dan membangun budaya industri fintech yang baik dan layanan keuangan digital. Hal ini dilakukan dengan memprioritaskan prinsip-prinsip tata kelola yang baik, termasuk melalui implementasi pedoman perilaku untuk operator *fintech* (Wawancara 2, 2022).

AFTECH memiliki Dewan Kehormatan/Etik yang bertugas dan berwenang untuk mengawasi pencapaian implementasi Kode Etik oleh anggota AFTECH, berhak untuk menerima dan mengkaji keluhan, serta menjatuhkan sanksi kepada anggota asosiasi yang dianggap telah melanggar Kode Etik asosiasi. Prosedur dan mekanisme proses pemeriksaan dan pengenaan sanksi yang berhubungan dengan pelanggaran Kode Etik diatur lebih lanjut dalam peraturan internal dan Standar Operasional Prosedur (SOP) Dewan Kehormatan/Etik.

Apabila terdapat anggota asosiasi yang terbukti telah melanggar Kode Etik atau tidak melaksanakan tugasnya, asosiasi akan mengambil langkah-langkah berikut ini:

1. Dewan Kehormatan/Etik menerima kasus pelanggaran Kode Etik asosiasi yang berasal dari:
 - a) permintaan regulator, yakni OJK atau BI;
 - b) keluhan tertulis dari anggota asosiasi; dan
 - c) pengawasan AFTECH atas perusahaan-perusahaan yang terdaftar sebagai perusahaan Inovasi Keuangan Digital di OJK.
2. Dewan Kehormatan/Etik menelusuri fakta-fakta terkait dugaan pelanggaran Kode Etik disertai oleh bukti yang meyakinkan bahwa telah terjadi dugaan pelanggaran Kode Etik asosiasi oleh anggota AFTECH.
3. Dewan Kehormatan/Etik akan memanggil secara tertulis anggota AFTECH yang diduga melanggar Kode Etik dalam kurun waktu 14 hari kerja setelah menemukan fakta dugaan pelanggaran Kode Etik, yakni untuk memeriksa dan mengonfirmasi kebenaran dugaan tersebut dan memberikan kesempatan bagi pihak yang bersangkutan untuk menyampaikan penjelasan dan pembelaannya. Pemanggilan tersebut harus dilakukan maksimal 7 (tujuh) hari kerja sebelum hari pemeriksaan.

Berdasarkan hasil pemeriksaan, apabila Dewan Kehormatan/Etik menemukan bahwa anggota asosiasi yang diperiksa terbukti telah melanggar Kode Etik, Dewan Kehormatan/Etik berhak menjatuhkan sanksi dalam bentuk:

- a) peringatan;
- b) pencabutan sementara keanggotaan AFTECH; atau
- c) pencabutan permanen keanggotaan AFTECH.

Pencabutan keanggotaan dapat memiliki konsekuensi yang serius terhadap perusahaan. Peraturan OJK mewajibkan semua perusahaan yang terdaftar untuk menjadi anggota asosiasi resmi. Kehilangan keanggotaan berarti melanggar persyaratan OJK, sehingga OJK dapat mencabut izin usaha perusahaan tersebut. Dengan kata lain, Kode Etik AFTECH bukan hanya lebih kuat dari sekadar wewenang komunitas, tetapi juga berdampak pada izin perusahaan anggota untuk beroperasi di pasar.

Kotak 3. Studi Kasus RupiahPlus

AFTECH, yang pada tahun 2019 mengalihkan kewenangan sebagai SRO khusus di bidang *fintech lending* kepada AFPI, juga telah memainkan peran dalam menutup kesenjangan regulasi dan pengawasan dalam ranah pinjaman *fintech*. Kasus besar pertama yang melibatkan privasi data dan penagihan utang terjadi pada Juni 2018. RupiahPlus, yang saat itu adalah pemberi pinjaman jangka pendek yang terdaftar di OJK, memiliki aplikasi yang memungkinkan operatornya untuk mengakses daftar kontak peminjam dan memanfaatkan akses ini untuk menagih utang ketika peminjam gagal melunasinya. RupiahPlus akan menghubungi orang-orang dalam daftar kontak peminjam dan memberitahukan kepada mereka tentang ketidakmampuan peminjam untuk melunasi utang, yakni untuk mendiskreditkan atau mempermalukannya (Sari, 2018). Belakangan ditemukan bahwa praktik ini tidak hanya dilakukan oleh RupiahPlus—hampir semua pemberi pinjaman jangka pendek, baik yang terdaftar di OJK maupun tidak, menggunakan praktik ini. Peminjam memberi izin pemberi pinjaman untuk mengakses daftar kontak mereka ketika mereka mengunduh aplikasi, tetapi tidak jelas apakah secara hukum diperlukan juga konsen dari setiap orang yang ada di dalam daftar kontak tersebut. Masih belum jelas juga apakah panggilan yang dilakukan untuk mempermalukan peminjam termasuk sebagai “perundungan” atau pelecehan.

Ketika kasus ini muncul, OJK dan AFTECH belum siap menghadapi situasi tersebut. Antara Juli–September 2018, OJK dan AFTECH melakukan serangkaian dengar pendapat dan konsultasi untuk memeriksa apakah tindakan tersebut melanggar hukum atau pedoman perilaku asosiasi. Dalam sebuah rapat yang dipimpin oleh OJK awal Juli 2018, RupiahPlus mengakui kesalahan mereka dan berjanji untuk memperbaiki keadaan. OJK selanjutnya meminta AFTECH untuk mempercepat proses pembuatan aturan tentang pinjaman yang bertanggung jawab, termasuk merinci praktik-praktik privasi yang bertanggung jawab – yang saat itu masih belum ada. Saat itu, aturan untuk memeriksa pelanggaran anggota dan komite independen untuk menyelidiki kasus juga belum dibuat oleh AFTECH. Berdasarkan permintaan dari OJK, AFTECH menyelidiki praktik yang dijalankan oleh RupiahPlus secara informal, yang dilakukan oleh anggota dewan yang relevan, dan selanjutnya oleh tim yang berisi pengacara independen, bersamaan dengan investigasi yang dilakukan oleh OJK sendiri. Temuan-temuan AFTECH digunakan untuk melengkapi temuan-temuan OJK, yang berujung pada pengenaan sanksi terhadap RupiahPlus. Akhirnya, pada 26 Juli 2018, OJK memutuskan untuk melarang RupiahPlus mengajukan izin selama tiga bulan (Pitoko, 2018).

Hanya beberapa hari sebelum sanksi dikenakan, pada 24 Juli 2018, AFTECH selesai menyusun pedoman perilaku untuk pinjaman yang bertanggung jawab, yang mengatur praktik-praktik pinjaman terbaik secara lebih teknis, termasuk tentang privasi data dan penagihan utang. Pedoman ini telah dibuat sejak April 2018 dan menerima umpan balik tertulis beberapa kali dari Departemen Perlindungan Konsumen OJK. Tekanan dari masyarakat yang mengerubungi kasus RupiahPlus juga memicu OJK memberikan izin kepada AFTECH untuk menerbitkan pedoman perilaku. Pedoman perilaku ini mewajibkan perusahaan *fintech*/penyedia layanan keuangan digital untuk beritikad baik dalam mengumpulkan, menyimpan, dan menggunakan data pribadi pengguna atau calon pengguna. Contoh-contoh penggunaan data pribadi yang tidak beritikad baik antara lain:

1. Meminta data pribadi dari calon pengguna tanpa bertujuan untuk memberikan layanan kepadanya
2. Mengumpulkan data pribadi yang tidak relevan dengan layanan yang ditujukan
3. Mengumpulkan data pribadi di luar data yang diberikan konsen oleh pengguna
4. Mengumpulkan data pribadi tanpa memiliki kapasitas untuk menangani data secara reliabel

Pedoman perilaku ini (selanjutnya direvisi oleh AFTECH pada tahun 2019 dan 2021, dan oleh AFPI pada tahun 2020⁵) menjadi dasar bagi asosiasi untuk mengawasi anggota-anggotanya, menerima keluhan konsumen, dan menjatuhkan sanksi kepada anggota yang tidak patuh. Sanksi yang diberikan dapat berupa peringatan formal hingga pencabutan keanggotaan. Ketika keanggotaan suatu perusahaan dicabut, OJK dapat menggunakan ini sebagai dasar pencabutan izin usaha platform yang bersangkutan.

Kasus ini menjadi bentuk awal bagaimana asosiasi industri dapat memainkan peran penting dalam menindak pelanggaran privasi. AFTECH sebagai lembaga industri, tanpa memiliki kerangka kerja yang jelas dan dengan permintaan dari OJK, melengkapi investigasi OJK melalui "percobaan oleh sesama (*trial by peers*)" untuk menentukan apakah tindakan suatu perusahaan dianggap sebagai norma atau praktik usaha yang lazim. Percobaan ini didukung oleh keberadaan pengacara-pengacara independen yang dapat memberikan wawasan dari segi hukum. Pada Oktober 2018, AFTECH memutuskan untuk memformalkan aturan-aturan tersebut untuk memastikan keadilan dan ketidakberpihakan proses pendisiplinan sesama (*peer discipline*), sembari menyediakan prosedur untuk mengescalasi ke komite independen.

⁵ Pedoman perilaku terbaru dari AFPI dapat diakses di sini: <https://www.afpi.or.id/articles/detail/pedoman-perilaku-afpi#>

LANGKAH SELANJUTNYA: POTENSI PERAN ASOSIASI PETUGAS PERLINDUNGAN DATA (DPO) DALAM PENGATURAN BERSAMA

Meski telah terdapat praktik-praktik di sektor keuangan digital yang dapat menjadi fondasi pengaturan bersama dalam perlindungan data pribadi, RUU PDP membuka peluang yang cukup besar bagi asosiasi DPO untuk memainkan peran dalam menegakkan aturan profesi, standar etik, dan standar kualifikasi atau kompetensi dalam perlindungan data pribadi. Peran ini berpotensi meningkatkan standar perlindungan data pribadi dengan berfokus pada aturan dan penerapannya pada individu dan di tingkat dewan pengurus atau manajemen (misal: DPO dalam perusahaan) untuk melengkapi tanggung jawab dan kewajiban di tingkat perusahaan.

Petugas Perlindungan Data (DPO) dalam RUU PDP dan Peraturan-Peraturan Lainnya

Petugas Perlindungan Data (*Data Protection Officer* atau DPO) merupakan bagian penting dari ekosistem perlindungan data yang sedang dicoba untuk dibangun oleh Kemenkominfo. Upaya ini diakui oleh Rencana Strategis Kemenkominfo 2020-2024 yang meliputi “pengembangan ekosistem DPO” sebagai salah satu prioritas Kemenkominfo. Kemenkominfo ingin menciptakan kerangka regulasi dimana asosiasi DPO dapat berkontribusi secara optimal terhadap pengembangan ekosistem DPO (Kemenkominfo, 2021).

Meski istilah DPO di Indonesia dipopulerkan oleh RUU PDP, pentingnya profesi spesialis pengelola data pribadi di ruang digital telah lama menjadi perhatian. “Narahubung (*contact person*)” yang bertanggung jawab mengatasi kekhawatiran pemilik data mengenai pengumpulan dan pengelolaan data pribadi mereka pertama kali disebutkan dalam Pasal 28 Permenkominfo No. 20/2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo No. 20/2016). Peran ini lebih lanjut diperluas dalam draf RUU PDP.

Dalam RUU PDP, peran dan tanggung jawab DPO berkaitan erat dengan tanggung jawab hukum prosesor dan pengendali data pribadi.⁶ Baik prosesor maupun pengendali data pribadi bertanggung jawab menangani data pribadi berkenaan dengan privasi individu dan hak pemilik data. Maka dari itu, prosesor dan pengendali data dimandatkan untuk menggunakan dan memproses data pribadi secara bertanggung jawab, transparan, dan terbatas. DPO membantu pengendali dan pengendali data menjalankan peran ini sesuai dengan peraturan perlindungan data yang berlaku.

Akan tetapi, tidak semua pengendali dan prosesor data diwajibkan untuk menunjuk DPO. RUU PDP mengadopsi pendekatan berbasis risiko seperti pendekatan yang digunakan dalam *European Union General Data Protection Regulation* (GDPR)—peraturan ini mendorong prosesor

⁶ Sesuai dengan kerangka kerja umum, pengendali data memiliki kendali penuh atas tujuan dan cara pemrosesan data pribadi, sementara prosesor data biasanya adalah pihak ketiga yang memproses data pribadi mewakili pengendali data.

dan pengendali data untuk menerapkan langkah-langkah protektif sesuai dengan tingkat risiko dari kegiatan penanganan datanya. Oleh karena itu, penunjukan DPO hanya dimandatkan untuk prosesor dan pengendali data yang terlibat dalam kegiatan-kegiatan berikut ini:

- a. Pemrosesan data pribadi untuk kepentingan pelayanan publik;
- b. Pengawasan data pribadi secara teratur dan sistematis berskala besar; dan
- c. Pemrosesan skala besar untuk data pribadi yang bersifat spesifik dan/atau data pribadi yang berhubungan dengan tindak pidana.

Draf RUU PDP menggunakan istilah Pejabat atau Petugas Pelindung Data Pribadi (PPPDP) untuk merujuk kepada DPO. Kata “pejabat” menandakan bahwa institusi publik yang memproses dan mengendalikan data pribadi juga dimandatkan untuk menunjuk DPO untuk membantu mereka memenuhi kewajiban institusionalnya.

Menurut Pasal 46 RUU PDP, peran-peran DPO meliputi:

- a. Menginformasikan dan memberikan saran untuk pengendali data pribadi atau prosesor data pribadi agar mematuhi ketentuan dalam Undang-Undang ini;
- 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;
- c. Memberikan saran mengenai penilaian dampak perlindungan data pribadi dan memantau kinerja pengendali data pribadi dan prosesor data pribadi; dan
- d. Berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan data pribadi, termasuk melakukan konsultasi mengenai mitigasi risiko dan/atau hal lainnya.

Peran dan Akuntabilitas DPO

Dalam draf RUU PDP versi termutakhir yang dapat diakses secara publik, rincian mengenai akuntabilitas, sanksi, dan tanggung jawab DPO dalam setiap tahapan siklus data masih belum dapat ditemukan. Salah satu interpretasi atas ketiadaan sanksi dan akuntabilitas dalam RUU PDP mirip dengan GPDR, karena DPO hanya akan menjalankan peran konsultasi untuk pengendali dan prosesor, dan sanksi untuk kegagalan memenuhi standar perlindungan akan dijatuhkan kepada pengendali dan prosesor data, bukan DPO (Kotak 1). Hal ini akan memengaruhi peran asosiasi DPO terkait pedoman perilaku untuk para profesional DPO, yang akan dijelaskan di bab selanjutnya.

Namun, terdapat perbedaan pemilihan kata yang mencolok antara RUU PDP dengan GPR ketika menyangkut soal DPO. Pasal 38 GDPR menyatakan bahwa DPO “memastikan”, sedangkan Pasal 45 RUU PDP menyatakan bahwa PPPDP “melaksanakan” fungsi perlindungan data pribadi. Menurut Kemenkominfo (2021), ini berarti bahwa, alih-alih hanya bertindak sebagai konsultan, PPPDP harus melaksanakan segala fungsi perlindungan data pribadi, yang meliputi kepatuhan hukum, tata kelola, manajemen, dan fungsi teknis. Meski demikian, rincian peran dan tanggung jawab DPO diharapkan akan diatur dalam peraturan pelaksana PDP.

Pelatihan dan Sertifikasi DPO

Meski Pasal 45 RUU PDP menyatakan bahwa DPO harus ditunjuk berdasarkan kualitas profesional, pengetahuan mengenai hukum dan praktik perlindungan data pribadi, dan kemampuan untuk memenuhi tugas-tugasnya, mekanisme yang menjelaskan bagaimana seseorang dapat memenuhi kualitas tersebut masih belum dibahas dalam draf RUU PDP terbaru, begitu pula dalam peraturan perundang-undangan lainnya di Indonesia. Rencana Strategis Kemenkominfo 2020-2024 menyiratkan bahwa aturan dan peraturan pelaksana tentang standardisasi DPO akan mengikuti setelah RUU PDP disahkan. Seberapa jauh asosiasi DPO dapat berperan dalam mengatur bersama profesi DPO masih terus menjadi bahan pembahasan.

Kualitas profesional yang disebut dalam Pasal 45 RUU PDP memiliki dimensi idealistis dan dimensi institusional (Simon, 2003). Dimensi idealistis memandang DPO sebagai sebuah profesi yang secara sukarela berkomitmen terhadap kepentingan klien dan nilai publik. Dimensi institusional menjajaki cara-cara untuk mengatur dan mendukung ekspektasi-ekspektasi yang ideal ini terhadap DPO, termasuk peran asosiasi profesi untuk secara mandiri meregulasi perilaku etis dan mengembangkan mekanisme untuk mempertahankan kualitas profesional anggota-anggotanya.

Regulasi mandiri yang dilakukan oleh asosiasi umumnya dimanifestasikan dalam bentuk pedoman praktik, sistem akreditasi berbasis industri, dan adopsi standar teknis secara sukarela (Hepburn, 2009). Tetapi, dikarenakan RUU PDP memberikan sedikit klarifikasi mengenai opsi mana yang akan diadopsi untuk mendukung kualitas DPO, seberapa jauh asosiasi DPO dapat berperan dalam mengatur bersama profesi DPO masih menjadi diskusi.

Model-model sertifikasi profesi

Bagaimana pun, peraturan perundang-undangan di Indonesia telah berupaya melibatkan asosiasi untuk memastikan tingkat profesionalisme tertentu di sejumlah lini pekerjaan. UU No. 18/2003 tentang Advokat, misalnya, menetapkan persyaratan minimal bagi seseorang untuk dapat dikatakan layak sebagai pengacara dan menjalankan perannya di dalam dan di luar pengadilan. Untuk bisa menjadi advokat, seseorang harus menjalani tahapan pendidikan wajib—mereka harus memiliki gelar Sarjana dari fakultas hukum, fakultas syariah, perguruan tinggi hukum militer, dan perguruan tinggi ilmu kepolisian⁷, sebelum dapat menyelesaikan pendidikan profesi hukum bernama Pendidikan Khusus Profesi Advokat (PKPA) dan lolos ujian profesi advokat. PKPA dijalankan oleh asosiasi advokat (serupa dengan asosiasi pengacara), yang menunjukkan adanya pembagian tanggung jawab antara aktor pemerintah dan non-pemerintah, yaitu asosiasi, dalam mempertahankan profesionalisme suatu profesi.

Profesi-profesi lain diatur secara berbeda melalui Sistem Pelatihan Kerja Nasional (SPKN) sebagaimana diatur oleh UU No. 13/2003 tentang Ketenagakerjaan (UU Ketenagakerjaan) jo. PP No. 31/2006 tentang Sistem Pelatihan Kerja Nasional (PP 31/2006). SPKN adalah mekanisme pelatihan profesi dan sertifikasi kompetensi oleh Badan Nasional Sertifikasi Profesi (BNSP)

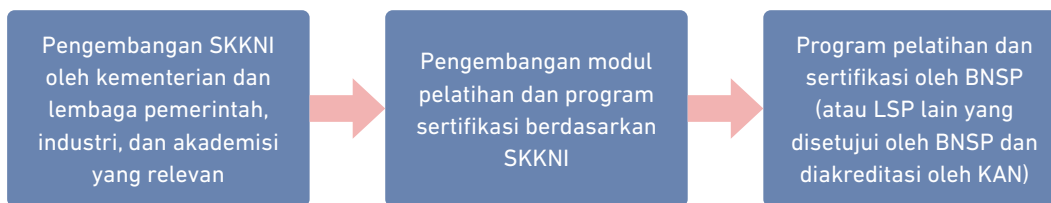
⁷ Pasal 2 (1) UU Advokat

atau Lembaga Sertifikasi Profesi (LSP) lainnya yang disetujui oleh BNSP. Skema ini mencakup sertifikasi profesi di berbagai sektor, termasuk layanan kesehatan dan kegiatan sosial, informasi dan komunikasi, konstruksi, persediaan air, dan pengelolaan sampah.

Mekanisme pelatihan dan sertifikasi ini harus mengikuti Standar Kompetensi Kerja Nasional Indonesia (SKKNI) yang meliputi persyaratan minimal pengetahuan, keterampilan, dan/atau keahlian dan sikap kerja yang relevan dengan pelaksanaan tugas dan persyaratan kerja. Lembaga Sertifikasi Profesi yang ingin menjalankan program pelatihan dan sertifikasi berdasarkan Standar Kompetensi Kerja Nasional Indonesia dapat mengajukan permohonan akreditasi kepada Komite Akreditasi Nasional (KAN) dengan merujuk kepada prosedur dalam UU No. 20/2014 tentang Standardisasi dan Penilaian Kesesuaian.

Di sektor TIK, Permenkominfo No. 24/2015 tentang Pemberlakuan Standar Kompetensi Kerja Nasional Indonesia Bidang Komunikasi dan Informatika (Permenkominfo No. 24/2015) telah menetapkan beberapa aturan dasar, yang salah satunya memandatkan lembaga publik maupun swasta di sektor TIK untuk memiliki pekerja yang bersertifikasi di bawah SKKNI.⁸ Ada 52 Standar Kompetensi Kerja Nasional Indonesia yang dikembangkan oleh Kemenkominfo di bawah skema Sistem Pelatihan Kerja Nasional (Kemenkominfo, 2021). Maka dari itu, adalah hal yang sangat mungkin untuk mengembangkan standar, kompetensi, dan sertifikasi DPO sebagai subsektor di bawah kerangka kerja ini.

Gambar 4.
Mekanisme Pelatihan dan Sertifikasi Kompetensi di bawah SPKN



Sumber: Analisis penulis

Di bawah skema ini, asosiasi DPO dapat turut mengembangkan SKKNI dalam subsektor perlindungan data. Asosiasi juga dapat mengajukan permohonan kepada BNSP dan KAN untuk disetujui sebagai LSP agar dapat menjalankan program sertifikasi dan pelatihan untuk DPO. Direktorat Tata Kelola Aplikasi Informatika juga akan terlibat dalam setiap prosesnya. Untuk memastikan bahwa ini tidak akan menjadi beban untuk perusahaan-perusahaan *startup* teknologi baru, persyaratan bertingkat dapat diterapkan untuk memberlakukan peraturan hanya untuk perusahaan-perusahaan tertentu, misalnya berdasarkan ukuran perusahaan atau jumlah data yang dikelola.

Menurut Kemenkominfo (2021, hal. 151), SKKNI akan dirancang berdasarkan *ASEAN Qualification on Reference Framework (AQR)* menggunakan format standar *International Labor Organization (ILO)* guna mematuhi standar global yang telah diakui.

⁸ Menurut Pasal 6 Permenkominfo No. 24/2015, ini bersifat kondisional tergantung dari ketersediaan setidaknya dua LSP di setiap subsektor SKKNI.

Meski RUU PDP tidak memberikan banyak rincian mengenai apakah DPO akan wajib tersertifikasi, dan jika pun demikian, mekanisme sertifikasi apa yang akan diterapkan dan pemangku kepentingan pemerintah dan non-pemerintah apa saja yang akan terlibat, Asosiasi Profesional Privasi Data Indonesia telah mulai menjalankan program pelatihan dan mengeluarkan sertifikat DPO di akhir pelatihannya. Mereka juga menawarkan keanggotaan berbayar, dengan manfaat-manfaat lain seperti acara tentang perlindungan data dan sumber daya untuk anggotanya. Karena masih belum ada peraturan yang menjadi dasar program sertifikasi, keikutsertaan dalam program ini tidak akan memengaruhi legalitas seseorang dalam menjalankan perannya sebagai DPO. Namun, ini dapat berguna bagi pengembangan profesional individu dan memberikan nilai jual tambah sebagai profesional perlindungan data.

Keanggotaan Asosiasi dan Peran Etik

Asosiasi DPO juga dapat berkontribusi terhadap ekosistem perlindungan data dengan merumuskan pedoman perilaku profesional demi memastikan bahwa DPO mempertahankan profesionalisme tinggi dalam menjalankan tugasnya. Area-area yang dapat termasuk dalam pedoman perilaku ini meliputi tanggung jawab DPO kepada klien dan pemberi kerjanya, komitmen terhadap kepatuhan hukum dan kepentingan publik, ketidakberpihakan, dan upaya pengembangan diri—yang kesemuanya relatif belum dijelaskan secara gamblang dalam RUU PDP.

Tetapi, jika keanggotaan asosiasi dan sertifikasi formal tidak diwajibkan oleh peraturan, penerapan pedoman perilaku dan insentif anggota untuk mematuhi akan menjadi kurang optimal. Berbeda dengan UU No. 18/2003 yang menjelaskan bahwa advokat wajib mematuhi kode etik organisasi advokat dengan risiko izin dicabut apabila tidak patuh, tidak ada ketentuan mengenai hal ini untuk DPO di dalam RUU PDP. Untuk saat ini, baik Asosiasi Praktisi Perlindungan Data Indonesia maupun Asosiasi Profesional Privasi Data Indonesia—dua asosiasi DPO teraktif di Indonesia—belum memiliki kode etik untuk anggota-anggotanya.

Kotak 4. Asosiasi Praktisi Perlindungan Data Indonesia

Asosiasi DPO merupakan platform komunikasi bagi praktisi-praktisi perlindungan data di Indonesia

Asosiasi Praktisi Perlindungan Data Indonesia adalah salah satu asosiasi DPO di Indonesia yang terdaftar di Kementerian Hukum dan Hak Asasi Manusia. Tujuan pertamanya dan yang terpenting adalah untuk menyediakan platform komunikasi bagi profesional-profesional DPO dan menjadi narahubung antar pemangku kepentingan terkait pengembangan kebijakan perlindungan data di Indonesia. Asosiasi ini menawarkan keanggotaan gratis untuk praktisi data di berbagai sektor digital.

Sejauh ini, Asosiasi Praktisi Perlindungan Data Indonesia telah mengadakan beberapa seminar dan pelatihan perlindungan data dengan tema yang umum maupun spesifik berdasarkan industri. Topiknya disesuaikan dengan kebutuhan anggota-anggotanya

dan topik relevan lain yang dapat meningkatkan pemahaman dan kesadaran seputar kegiatan data digital selaras dengan peraturan perundang-undangan yang berlaku di Indonesia. Asosiasi ini menghadirkan ahli-ahli industri untuk berbicara dengan anggota-anggotanya mengenai aneka topik seputar privasi.

Terkait wewenang regulasi mandiri asosiasi ini untuk mengembangkan kode etik bagi anggota-anggotanya, perwakilan asosiasi mengatakan bahwa mereka akan menunggu perkembangan RUU PDP dan melihat apakah kode etik bagi anggota akan sesuai dengan ekosistem DPO yang sedang dibangun oleh Kemenkominfo.

Sikap serupa juga diungkapkan berkenaan dengan sertifikasi DPO oleh asosiasi. Berbeda dengan Asosiasi Profesional Privasi Data Indonesia yang telah mulai menjalankan program-program pelatihan dan sertifikasi, Asosiasi Praktisi Perlindungan Data Indonesia memilih menunggu keputusan apakah mekanisme tersebut akan didukung oleh UU PDP nantinya.

Latar belakang yang beragam dalam profesi privasi juga menghadirkan sebuah tantangan dalam membuat pedoman perilaku. Profesi privasi diisi dengan para ahli teknologi, insinyur, dan pengacara, yang masing-masing memiliki perspektifnya sendiri terhadap peraturan perlindungan data. Lebih lanjut lagi, karena RUU PDP memposisikan DPO sebagai konsultan bagi pengendali dan prosesor data, terdapat isu akuntabilitas DPO—sejauh mana DPO bertanggung jawab atas pelanggaran data oleh pengendali atau prosesor data, dan bagaimana pedoman perilaku dapat mencerminkan akuntabilitas ini.

Ketika terjadi kasus pelanggaran data, dengan kerangka regulasi yang ada di Indonesia untuk perlindungan data pribadi, APPDI melihat bahwa tanggung jawab berada di tangan tim manajemen, bukan DPO (Wawancara 1, 2022). Hal ini dikarenakan DPO berperan sebagai penasihat tim manajemen perusahaan atau lembaga, atau dalam kasus ini yaitu pengendali data. Pada akhirnya, tim manajemenlah yang memiliki kebebasan untuk memutuskan apakah saran DPO diterima atau tidak dalam menanggapi kasusnya. Maka dari itu, tanggung jawab utama DPO adalah memberi saran dan memastikan bahwa pengendali data mematuhi hukum.

Latar belakang yang beragam dalam profesi privasi juga menghadirkan sebuah tantangan dalam membuat pedoman perilaku.

Perbandingan dengan GDPR

Serupa dengan RUU PDP, peran DPO dalam GDPR berkaitan erat dengan kewajiban pengendali dan prosesor data untuk mematuhi standar dan persyaratan tertentu dalam kegiatan data mereka. Pasal 37 GDPR memandatkan pengendali dan prosesor data untuk menunjuk DPO dalam kegiatan-kegiatan yang melibatkan pemrosesan data pribadi berskala besar dalam kategori-kategori khusus, pengawasan subjek data berskala besar secara teratur dan sistematis, dan pemrosesan data oleh otoritas publik.

Lebih lanjut lagi, Pasal 39 GDPR menekankan bahwa DPO harus ditunjuk berdasarkan “kualitas profesional”, dan khususnya “pengetahuan ahli tentang hukum dan praktik perlindungan data” untuk memenuhi tugasnya sebagaimana termaktub dalam Pasal 39 GDPR.

Selain ketentuan-ketentuan yang ada dalam GDPR, Uni Eropa (UE) juga mengeluarkan *Guidelines⁹ on Data Protection Officers* (Pedoman Petugas Perlindungan Data) (2017) dimana pengendali dan prosesor data pribadi didorong untuk mempertimbangkan kualifikasi-kualifikasi berikut ini dalam menunjuk DPO:

- kepakaran terkait hukum dan praktik perlindungan data nasional dan Eropa, termasuk pemahaman mendalam seputar GDPR;
- pemahaman seputar operasi pemrosesan yang dilakukan;
- pemahaman seputar teknologi informasi dan keamanan data;
- pengetahuan seputar sektor bisnis dan organisasi; dan
- kemampuan untuk mempromosikan budaya perlindungan data dalam organisasi

Sesuai dengan Pasal 39 Ayat 2 GDPR yang menekankan bahwa DPO harus mempertimbangkan tingkat-tingkat risiko yang berhubungan dengan sifat, lingkup, konteks, dan tujuan operasi pemrosesan data, tingkat pengetahuan ahli yang dibutuhkan harus ditentukan berdasarkan operasi pemrosesan data pribadi yang dilakukan serta perlindungan yang dibutuhkan untuk data tersebut. Contohnya, kegiatan pemrosesan data yang kompleks, atau yang melibatkan data sensitif dalam jumlah besar, membutuhkan DPO dengan tingkat kepakaran yang lebih tinggi (UE, 2017).

Namun, GDPR tidak memandatkan sertifikasi atau kualifikasi formal apa pun bagi seseorang untuk menjadi DPO. Dalam praktiknya, organisasi privasi seperti *International Association of Privacy Professionals* (IAPP) telah terlibat dalam berbagai kegiatan pendukung untuk DPO, termasuk menawarkan kursus dan sertifikasi yang relevan dengan peran dan tanggung jawab DPO, seperti *Certified Information Privacy Professional* (CIPP), *Certified Information Privacy Manager* (CIPM), dan *Certified Information Privacy Technologist* (CIPT). Kredensial-kredensial ini diakreditasi oleh *American National Standards Institute* (ANSI) di bawah standar *International Organization for Standardization* (ISO) 17024: 2012—untuk memastikan bahwa kredensial-kredensial ini diakui secara global.

Otoritas Perlindungan Data di Prancis, *Commission nationale de l’informatique et des libertés* (CNIL) mengambil beberapa langkah ekstra untuk memfasilitasi sertifikasi DPO. Sejak 2018, CNIL telah mengizinkan organisasi-organisasi pihak ketiga untuk mengeluarkan sertifikasi keterampilan DPO, dan menyimpan daftar organisasi-organisasi tersebut (CNIL, t.t.). Sertifikasi

⁹ Pedoman ini dapat diakses di: <https://ec.europa.eu/newsroom/article29/items/612048>

ini hanya dapat diikuti setelah memiliki dua tahun pengalaman dalam perlindungan data, atau dua tahun di bidang apa pun dengan setidaknya 35 jam pelatihan tentang perlindungan data (CNIL, t.t.). Masa berlaku sertifikasi adalah tiga tahun.

Sertifikasi ini, meski tidak wajib untuk menjadi DPO, membantu calon DPO maupun organisasi untuk mematuhi GDPR. Bagi calon DPO, sertifikasi menjadi bukti bahwa tingkat pengetahuannya memadai sesuai yang disyaratkan oleh Pasal 39 GDPR. Bagi organisasi, sertifikasi membantu menemukan individu yang layak untuk ditunjuk sebagai DPO.

DPO di Spanyol: Peran Sentral Lembaga Perlindungan Data

Di antara negara-negara anggota UE yang tunduk kepada GDPR, Spanyol mengambil sejumlah langkah ekstra dalam mengatur DPO—dengan mengembangkan skema sertifikasi di bawah pengawasan Lembaga Perlindungan Data Spanyol (*Agencia Española de Protección de Datos* atau AEPD). Bersama dengan Badan Akreditasi Nasional (*Entidad Nacional de Acreditación* atau ENAC), AEPD mengembangkan skema sertifikasi DPO dengan standar yang setara dengan ISO 17024 (IAPP, 2017).

Program sertifikasi dapat dilakukan oleh entitas yang memenuhi kriteria dan persyaratan yang ditetapkan oleh Skema Sertifikasi Petugas Perlindungan Data dari Lembaga Perlindungan Data Spanyol (Skema DPO-AEPD) (2017). Karena program ini didasarkan pada kompetensi dan kapasitas teknis, lembaga harus mendapatkan dan mempertahankan akreditasi dari ENAC untuk mengeluarkan sertifikasi kepada DPO sesuai dengan Skema DPO-AEPD. AEPD secara rutin memperbarui daftar lembaga sertifikasi yang terakreditasi dan memverifikasi kepatuhan mereka terhadap kewajibannya.

Berdasarkan Bagian 6.3. dari Skema DPO-AEPD, sebelum mengikuti ujian sertifikasi, calon DPO harus memenuhi salah satu prasyarat berikut ini:

1. Menunjukkan pengalaman profesional selama setidaknya lima tahun dalam proyek dan/atau kegiatan dan tugas yang berhubungan dengan fungsi DPO terkait perlindungan data;
2. Menunjukkan pengalaman profesional selama setidaknya tiga tahun dalam proyek dan/atau kegiatan dan tugas yang berhubungan dengan fungsi DPO terkait perlindungan data, dan setidaknya 60 jam pelatihan yang diakui tentang topik-topik yang berhubungan dengan program;
3. Menunjukkan pengalaman profesional setidaknya dua tahun dalam proyek dan/atau kegiatan dan tugas yang berhubungan dengan fungsi DPO terkait perlindungan data, dan setidaknya 100 jam pelatihan yang diakui tentang topik-topik yang berhubungan dengan program;
4. Menunjukkan setidaknya 180 jam pelatihan yang diakui tentang topik-topik yang berhubungan dengan program.

Selain merinci kualifikasi profesional untuk DPO, AEPD juga menyusun kode etik yang harus disepakati oleh calon DPO sebelum mengambil program sertifikasi.¹⁰ Kegagalan dalam mematuhi prinsip, nilai, dan kriteria dalam kode etik ini dapat berujung pada penangguhan atau penghapusan dari sertifikasi.

¹⁰ Bagian 6.4. jo. Annex III Skema DPO-AEPD

KESIMPULAN DAN REKOMENDASI KEBIJAKAN

Kementerian Komunikasi dan Informatika (Kemenkominfo) telah menyusun berbagai langkah untuk memastikan kesesuaian dengan praktik-praktik terbaik perlindungan data pribadi. Langkah-langkah tersebut meliputi pelaksanaan mekanisme yang tercantum dalam PP 71. Namun, seiring pertumbuhan eksponensial transaksi digital, muncul kebutuhan untuk melengkapi langkah-langkah ini dengan standar-standar dan langkah-langkah preventif yang spesifik berdasarkan sektor, serta melibatkan aktor non-negara dalam mekanisme pelaksanaannya. Di Indonesia, terutama dalam sektor jasa keuangan, asosiasi industri telah memainkan peran ini sebagai “organisasi regulator mandiri” yang melengkapi upaya pengawasan entitas-entitas yang termasuk dalam lingkup pengaturan.

Baru-baru ini, terdapat preseden untuk memperluas peran asosiasi ke ranah keuangan digital, termasuk jika terjadi pelanggaran perlindungan data pribadi. Kasus RupiahPlus pada tahun 2018 menghasilkan pedoman perilaku industri untuk keuangan digital yang bertanggung jawab, yang termasuk praktik-praktik terbaik perlindungan data pribadi, dan selanjutnya disempurnakan oleh pedoman perilaku industri terkait perlindungan data pribadi. Semua ini merupakan inisiatif asosiasi industri dengan dukungan penuh dari OJK sebagai regulator keuangan. Model ini dapat diadopsi untuk platform digital secara umum, dengan mengambil peluang dari RUU PDP yang dapat menerapkan struktur pendekatan pengaturan bersama yang serupa.

Sementara itu, meski organisasi DPO masih baru di Indonesia, praktik-praktik di negara-negara lain menunjukkan bahwa ia dapat menjadi mitra pengaturan bersama dalam menjaga ketaatan terhadap standar perlindungan data pribadi.

Dari Tabel 4 di bawah, CIPS mengidentifikasi tujuh asosiasi di sistem ekonomi digital Indonesia yang berhubungan dengan perlindungan data dan petugas perlindungan data. Daftar lengkap yang berisi nama-nama asosiasi dan komunitas teknologi informasi disediakan oleh Kemenkominfo di bawah Direktorat Jenderal Aplikasi Informatika (Kemenkominfo, 2019). Dengan pesatnya perkembangan di sektor ini, daftar asosiasi usaha dan profesi dapat bertambah dari yang disebutkan di makalah ini.

Tabel 4.
Daftar Asosiasi yang Berhubungan dengan Ekosistem Ekonomi Digital dan Petugas Perlindungan Data di Indonesia

No.	Nama Asosiasi	Singkatan	Jenis Asosiasi	Tahun Didirikan
1	Asosiasi Fintech Indonesia	AFTECH	Industri	2016
2	Asosiasi Fintech Pendanaan Indonesia	AFPI	Industri	2019
3	Asosiasi Fintech Syariah Indonesia	AFSI	Industri	2018
4	Asosiasi E-commerce Indonesia	idEA	Industri	2012
5	Asosiasi Sistem Pembayaran Indonesia	ASPI	Industri	2011
6	Asosiasi Praktisi Pelindungan Data Indonesia	APPDI	Profesi	2020
7	Asosiasi Profesional Privasi Data Indonesia	APPDI	Profesi	2020

Sumber: Analisis dan kompilasi penulis

Memanfaatkan praktik-praktik yang digunakan di organisasi-organisasi ini (dan organisasi baru apa pun nantinya), berikut adalah rekomendasi kami untuk perbaikan di masa mendatang:

- Mengizinkan dan memperkenankan asosiasi industri untuk memiliki fleksibilitas dalam mengembangkan standar-standar teknis sendiri yang spesifik berdasarkan sektornya. Hal ini meliputi urusan yang sangat teknis seperti pengumpulan dan pemrosesan data dalam biometrik, keuangan digital, kota cerdas/*Internet of Things*, dan banyak lainnya.
- Pengawasan regulasi diperlukan untuk memastikan bahwa asosiasi dan standar-standar ini diawasi dan diaudit dengan benar oleh otoritas regulasi. Dalam kasus PDP, otoritas yang bertugas adalah yang ditunjuk oleh RUU PDP.¹¹ Ini ditujukan untuk mendorong pengambilan keputusan yang demokratis dalam asosiasi, melakukan pemeriksaan dan keseimbangan (*checks and balances*), dan mencegah asosiasi dari tindakan “penawanan” oleh pelaku industri yang dominan dengan perilaku anti persaingan seperti membuat hambatan masuk bagi pelaku-pelaku baru. Interaksi antara regulator dengan asosiasi menjadi fondasi pengaturan bersama.
- Melakukan konsultasi regulasi secara rutin dalam urusan regulasi mandiri industri, seperti penyusunan pedoman perilaku. Regulator keuangan sudah melakukan ini, sebagaimana ditunjukkan oleh komunikasi yang intensif dalam penyusunan pedoman perilaku pinjaman atau standar pembayaran yang dilakukan selama proses pembuatan standar. Hal ini menciptakan keseimbangan yang dinamis antara kepentingan regulasi dan kepentingan komersial.
- Memfokuskan pengembangan standar teknis di tingkat profesional, atau dalam hal ini DPO sebagai profesi. Pengalaman di Eropa menunjukkan bahwa, meski tidak ada persyaratan DPO wajib, tingginya kualitas rincian teknis DPO yang dikeluarkan oleh UE atau lembaga perlindungan data nasional telah mendorong industri untuk mengadopsi standar-standar ini. Sebagai gantinya, pemerintah dapat menyetujui satu atau beberapa asosiasi DPO sebagai lembaga pembuat standar profesional di negaranya.
- Di tingkat regulasi, mendorong kolaborasi regulasi antara otoritas data (Kemenkominfo atau entitas apa pun yang ditunjuk oleh RUU PDP) dan regulator sektoral (OJK, BI, Kementerian Kesehatan, dll.) untuk membuat tolok ukur tertentu agar standar industri dapat sesuai dengan peraturan PDP dan peraturan yang spesifik di setiap sektor.

¹¹ Wewenang pengawasan dan regulasi atas data pribadi adalah salah satu topik yang paling diperdebatkan dalam RUU PDP. Meski pemerintah eksekutif lebih memilih Kemenkominfo sebagai regulator, DPR bersikeras untuk membuat lembaga independen yang baru. Hingga Juni 2022, isu dalam draf RUU PDP ini kemungkinan akan diserahkan kepada Presiden.

REFERENSI

- AEPD [Agencia Española de Protección de Datos]. (2017). *Certification Scheme of Data Protection Officers from the Spanish Data Protection Agency (DPO-AEPD Scheme)*. AEPD. Retrieved from <https://www.aepd.es/sites/default/files/2019-12/scheme-aepd-dpd.pdf>
- AFPI. (2019). *Pedoman Perilaku Pemberian Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi Secara Bertanggung Jawab*. Retrieved from <https://www.afpi.or.id/articles/detail/pedoman-perilaku-afpi#>
- AFTECH, AFPI, and AFSI. (2019). *Pedoman Perilaku Penyelenggara Teknologi Finansial di Sektor Jasa Keuangan yang Bertanggungjawab*. Retrieved from [https://fintech.id/storage/files/shares/Kode%20Etik/Joint%20CoC%20-%20AFTECH%20AFSI%20AFPI%20\[PUBLIC\].pdf](https://fintech.id/storage/files/shares/Kode%20Etik/Joint%20CoC%20-%20AFTECH%20AFSI%20AFPI%20[PUBLIC].pdf)
- AFTECH. (2021). *Kode Etik terkait Perlindungan Data Pribadi dan Kerahasiaan Data di Sektor Teknologi Finansial*. Retrieved from <https://fintech.id/storage/files/shares/Kode%20Etik/Kode%20Etik%20AFTECH%20-%20TF%20PDP.pdf>
- AFTECH. (n.d.). *Tentang Kami*. Retrieved from <https://fintech.id/id/about#working-group>
- Aprilianti, I & Dina, SA. (2021). *Co-regulating the Indonesian Digital Economy*. Center for Indonesian Policy Studies. Retrieved from <https://www.cips-indonesia.org/publications/co-regulating-the-indonesian-digital-economy>
- Audrine, P & Murwani, A. (2021). *Implementing the Digital Economy Enabling Environment Guide: A Case Study from Indonesia*. Center for Indonesian Policy Studies. Retrieved from <https://www.cips-indonesia.org/publications/implementing-the-digital-economy-enabling-environment-guide%3A-a-case-study-from-indonesia>
- CNIL [Commission nationale de l'informatique et des libertés]. (n.d.). *Practical Guide for Data Protection Officers*. Retrieved from https://www.cnil.fr/sites/default/files/atoms/files/cnil-gdpr_practical_guide_data-protection-officers.pdf
- Devi, Z.M. (2015). *idEA Bakal Terbitkan Kode Etik Khusus e-Commerce*. Marketeters. Retrieved from <https://www.marketeters.com/idea-bakal-terbitkan-kode-etik-khusus-e-commerce?amp=1>
- EU. (2017). *Guidelines on Data Protection Officers (DPOs)*. European Union. Retrieved from <https://ec.europa.eu/newsroom/article29/items/612048>
- Finck, M. (2017). *Digital Regulation: Designing a Supranational Legal Framework for the Platforms Economy*. LSE Law, Society and Economy Working Papers, 15/2017.
- Google, Temasek, & Bain & Company. (2021). *e-Conomy SEA 2021 Roaring 20s: The SEA Digital Decade*. https://www.bain.com/globalassets/noindex/2021/e_conomy_sea_2021_report.pdf
- Hepburn, G. (2018). *OECD Report: Alternatives to Traditional Regulation*.
- Hepburn, G., (2009). *Alternatives to traditional regulation. Report prepared for the OECD Regulatory Policy Division*. <https://www.oecd.org/gov/regulatory-policy/42245468.pdf>
- IAPP. (2017). *Here's what it takes to be a certified DPO in Spain*. IAPP. Retrieved from <https://iapp.org/news/a/heres-what-it-takes-to-be-a-certified-dpo-in-spain/#:~:text=Certification%20bodies'%20evaluators%20will%20need,years'%20experience%20in%20either%20data>
- Karunian. (2020). *Kawal Pembahasan RUU Pelindungan Data Pribadi, Koalisi Advokasi RUU PDP serahkan usulan DIM Alternatif kepada DPR RI*. Retrieved from: <https://elsam.or.id/kawal-pembahasan-ruu-pelindungan-data-pribadi-koalisi-advokasi-ruupdp-serahkan-usulan-dim-alternatif>
- Kemenkominfo [Kementerian Komunikasi dan Informatika]. (2019). *Komunitas TIK*. Retrieved from <https://aptika.kominfo.go.id/category/data-aptika/komunitas/>
- Kemenkominfo [Kementerian Komunikasi dan Informatika]. (2021). *Grand Design Pembentukan Data Protection Officer (DPO) Indonesia*, Directorate General of Information Technology Applications MOCI.

Pitoko, R.A. (2018). Dapat Sanksi, RupiahPlus Dilarang Ajukan Izin ke OJK selama Tiga Bulan. Kompas. Retrieved from <https://ekonomi.kompas.com/read/2018/07/26/192744126/dapat-sanksi-rupiahplus-dilarang-ajukan-izin-ke-ojk-selama-tiga-bulan?page=all>.

Riyadi, G. (2021). Data Privacy in the Indonesian Personal Data Protection Legislation. Center for Indonesian Policy Studies. <https://www.cips-indonesia.org/publications/data-privacy-in-the-indonesian-personal-data-protection-legislation>

Sari, F. (2018). OJK akan jatuhkan sanksi kepada fintech RupiahPlus. Kontan. Retrieved from <https://keuangan.kontan.co.id/news/ojk-akan-jatuhkan-sanksi-fintech-rupiah-plus>

Setiawan, K. (2020). Bos OJK Hampir Setiap Hari Terima Surat Komplain Soal Fintech. Tempo Bisnis 18 November 2020. Retrieved from <https://bisnis.tempo.co/read/1406552/bos-ojk-hampir-setiap-hari-terima-surat-komplain-soal-fintech/full&view=ok>

Simon, William. (2003). 'Who Needs the Bar?: Professionalism Without Monopoly', Florida State University Law Review, Vol. 30 (4), pp.639-658

Suleiman, A. (2021). Improving Consumer Protection for Low-Income Customers in P2P Lending. Center for Indonesian Policy Studies. <https://www.cips-indonesia.org/publications/improving-consumer-protection-for-low-income-customers-in-p2p-lending>

Sutanto, T. (n.d.). Asosiasi Sistem Informasi Indonesia. Retrieved from http://aisindo.org/wp-content/uploads/2014/07/SistemInformasi_sebagai_PROFESI.pdf

Torring, J., Sørensen, E., & Røiseland, A. (2019). Transforming the public sector into an arena for co-creation: Barriers, drivers, benefits, and ways forward. Administration & Society, 51(5), 795-825.

Wawancara

Wawancara 1: Ketua & Wakil Asosiasi Praktisi Pelindungan Data Indonesia (2022, April). Komunikasi pribadi.

Wawancara 2: Wakil Sekretaris Jenderal & Kepala Gugus Tugas Perlindungan Data Pribadi Asosiasi Fintech Indonesia (2022, April). Komunikasi pribadi.

TENTANG PENULIS

Ajisatria Suleiman adalah Peneliti Mitra di Center for Indonesian Policy Studies. Ia merupakan praktisi bidang regulasi kebijakan publik dengan spesialisasi Ekonomi Digital dan Keuangan Digital. Dalam kariernya, ia telah membantu mengembangkan internet secara regional dan nasional, serta bekerja sama dengan asosiasi industri keuangan digital, badan pengembangan internasional, perusahaan teknologi berbasis global, dan perusahaan rintisan lokal. Fokus penelitiannya adalah perlindungan data pribadi, kedaulatan digital, dan keuangan digital. Ia mendapatkan gelar Sarjana Hukum dari Universitas Indonesia, dan gelar Master dari Erasmus University of Rotterdam dan University of Hamburg.

Pingkan Audrine adalah seorang Peneliti di Center for Indonesian Policy Studies dengan fokus penelitian di bidang Peluang Ekonomi. Pingkan memperoleh gelar Sarjana Ilmu Politik dari Universitas Katolik Parahyangan. Sebelum bergabung dengan CIPS, Pingkan memiliki pengalaman bekerja di radio swasta nasional, kantor internasional di lembaga pendidikan tinggi dan Kantor Kepala Perwakilan PBB di Indonesia.

Thomas Dewaranu memperoleh gelar master dalam kebijakan publik dari Australian National University dan gelar sarjana hukum dari Universitas Indonesia. Minat penelitiannya meliputi pembangunan pedesaan dan pengentasan kemiskinan. Sebelum bergabung dengan CIPS, ia bekerja di sebuah firma hukum komersial di Jakarta, memberikan layanan hukum kepada perusahaan lokal dan multinasional.

AYO BERGABUNG DALAM PROGRAM “SUPPORTERS CIRCLES” KAMI

Melalui *Supporters Circles*, kamu, bersama dengan ratusan lainnya, membantu kami untuk melakukan penelitian kebijakan serta advokasi untuk kemakmuran jutaan orang di Indonesia yang lebih baik.

Dengan bergabung dalam *Supporters Circles*, *supporters* akan mendapatkan keuntungan dengan terlibat lebih dalam di beberapa karya CIPS. *Supporters* bisa mendapatkan:

- Undangan Tahunan Gala Dinner CIPS
- Pertemuan eksklusif dengan pimpinan CIPS
- Mendapatkan prioritas pada acara-acara yang diadakan oleh CIPS
- Mendapatkan informasi terbaru secara personal, setiap satu bulan atau empat bulan, lewat email dan video mengenai CIPS
- Mendapatkan hard-copy materi publikasi CIPS (lewat permintaan)



Untuk informasi lebih lanjut, silahkan hubungi anthea.haryoko@cips-indonesia.org.

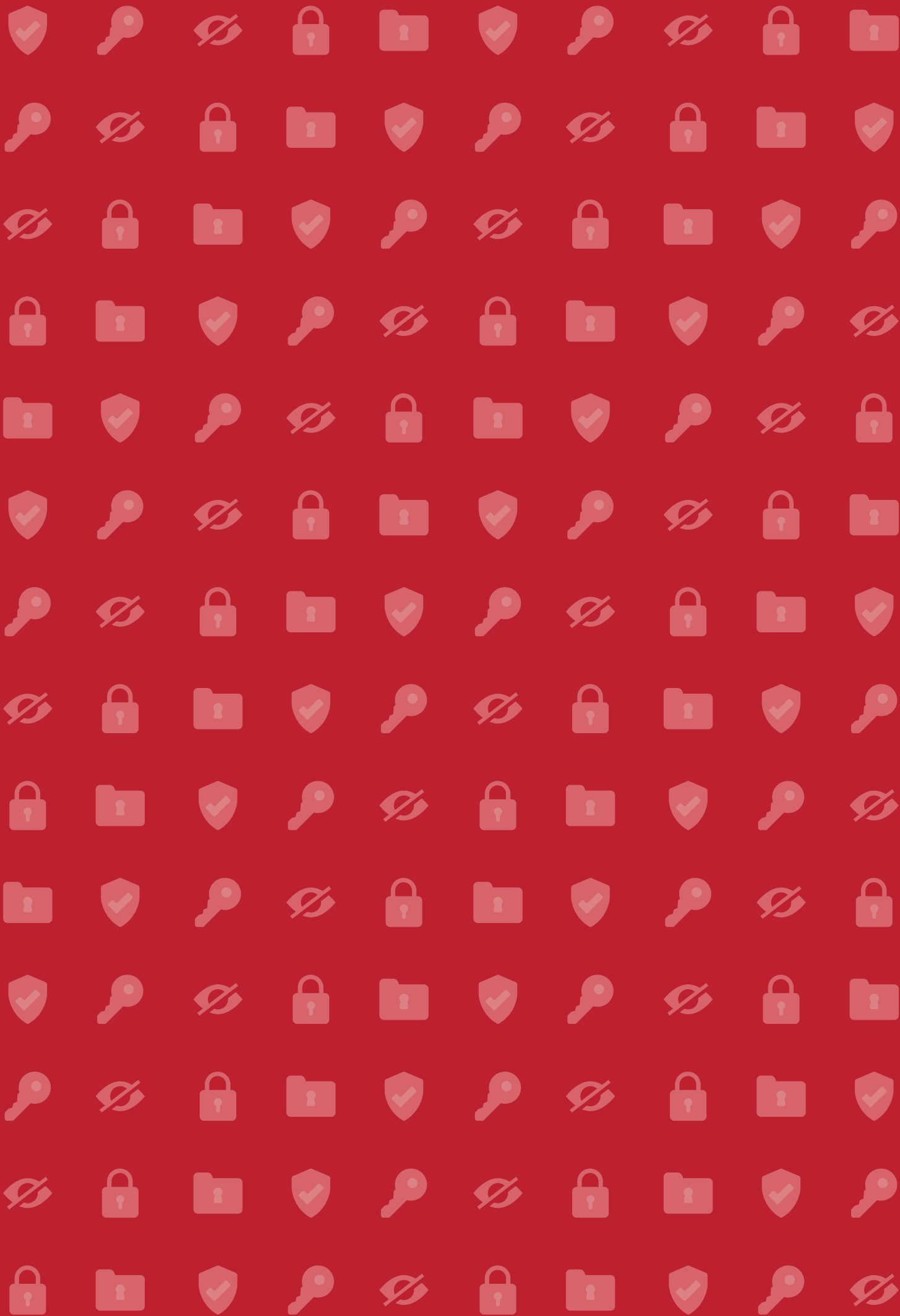


Pindai untuk bergabung









TENTANG CENTER FOR INDONESIAN POLICY STUDIES

Center for Indonesian Policy Studies (CIPS) merupakan lembaga pemikir non-partisan dan non profit yang bertujuan untuk menyediakan analisis kebijakan dan rekomendasi kebijakan praktis bagi pembuat kebijakan yang ada di dalam lembaga pemerintah eksekutif dan legislatif.

CIPS mendorong reformasi sosial ekonomi berdasarkan kepercayaan bahwa hanya keterbukaan sipil, politik, dan ekonomi yang bisa membuat Indonesia menjadi sejahtera. Kami didukung secara finansial oleh para donatur dan filantropis yang menghargai independensi analisis kami.

FOKUS AREA CIPS:


Ketahanan Pangan dan Agrikultur: CIPS terlibat dalam penelitian mengenai pertanian yang berkelanjutan dan modern. CIPS juga meneliti dan mengadvokasi alternatif kebijakan yang membuka perdagangan bahan pangan strategis untuk menstabilkan harga pangan dan mencapai ketahanan pangan bagi masyarakat Indonesia. Kami memaparkan hubungan antara pertanian, perdagangan dan investasi, harga pangan, dan pola makan bergizi konsumen Indonesia dengan tujuan memastikan bahwa keluarga berpenghasilan rendah dapat mengakses makanan berkualitas dengan harga terjangkau.


Pendidikan: CIPS melakukan penelitian dan advokasi kebijakan pendidikan di Indonesia untuk meningkatkan aksesibilitas dan kualitas pendidikan. Kami fokus pada bagaimana inisiatif swasta, otonomi sekolah yang lebih besar, dan keterampilan yang tepat di antara siswa dan guru dapat membangun sistem pendidikan yang tangguh di Indonesia, memfasilitasi peningkatan kualitas pendidikan dan meningkatkan pilihan pendidikan bagi masyarakat Indonesia yang berpenghasilan rendah.


Peluang Ekonomi: CIPS percaya bahwa kebebasan ekonomi yang lebih besar dan keterbukaan pasar dapat menghasilkan peluang ekonomi bagi masyarakat Indonesia untuk mengakses dan memperoleh kehidupan yang layak. Baik melalui perdagangan dan investasi, teknologi digital, kewirausahaan, hak milik, ataupun peluang kerja, CIPS mengadvokasi reformasi kebijakan yang memungkinkan masyarakat Indonesia dengan berbagai latar belakang untuk mendapatkan kemakmuran yang lebih besar bagi diri mereka sendiri dan komunitas mereka.


www.cips-indonesia.org

 facebook.com/cips.indonesia

 [@cips_id](https://twitter.com/cips_id)

 [@cips_id](https://www.instagram.com/cips_id)

 [Center for Indonesian Policy Studies](https://www.linkedin.com/company/center-for-indonesian-policy-studies)

 [Center for Indonesian Policy Studies](https://www.youtube.com/channel/UC...)

Jalan Terogong Raya No. 6B
Cilandak, Jakarta Selatan 12430
Indonesia