



14 September 2023

KOMENTAR BSA MENGENAI RANCANGAN PERATURAN PELAKSANAAN UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI

Pendahuluan

Atas nama BSA | The Software Alliance (**BSA**),¹ kami mengucapkan terima kasih karena telah meminta masukan dari pihak swasta terhadap Rancangan Peraturan Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (**Rancangan Peraturan PDP**). Kami menyambut baik kesempatan untuk menyampaikan komentar kepada Kementerian Komunikasi dan Informatika (**KOMINFO**). Di tahun-tahun sebelumnya, BSA telah memberikan komentar dalam pengajuan bersama: tentang Rancangan Undang-Undang Perlindungan Data Pribadi pada tahun 2019², dan Rancangan Perubahan Peraturan Pemerintah 82/2012 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik pada tahun 2018.³ Baru-baru ini di bulan Maret 2023, kami bertemu dengan pejabat dari KOMINFO di sela-sela *Initiative Indonesia Financial Services and Information Technology Mission*.

BSA adalah advokat terkemuka untuk industri perangkat lunak global. Anggota-anggota kami adalah perusahaan-perusahaan perangkat lunak yang menciptakan teknologi bisnis-ke-bisnis (*business-to-business*) yang membantu bisnis-bisnis lain berinovasi dan tumbuh. Sebagai contoh, anggota-anggota BSA menyediakan alat termasuk penyimpanan *cloud* dan layanan pemrosesan data, perangkat lunak manajemen hubungan pelanggan, program manajemen sumber daya manusia, layanan manajemen identitas, dan perangkat lunak kolaborasi. BSA menawarkan pengalaman global kami yang luas dalam hal kebijakan teknologi untuk dijadikan sumber daya, dan kami berharap komentar kami dalam pengajuan ini akan bermanfaat bagi KOMINFO.

Berikan waktu yang cukup untuk keterlibatan dengan sektor swasta

BSA kembali menegaskan Kembali apresiasi kami kepada KOMINFO yang telah melakukan konsultasi publik. Kami dengan hormat menyarankan untuk meningkatkan proses keterlibatan dengan memperpanjang jangka waktu untuk pemberian masukan publik. Apabila dibandingkan dengan yurisdiksi lain di kawasan ini — yang biasanya memberikan jangka waktu setidaknya satu hingga dua bulan untuk draf dokumen yang jauh lebih pendek — memberikan jangka waktu yang lebih panjang untuk melakukan peninjauan terhadap Rancangan Peraturan PDP yang ekstensif ini akan memfasilitasi pemeriksaan yang lebih rinci. Menetapkan periode konsultasi yang lebih panjang juga akan

¹ Anggota-Anggota BSA meliputi: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Palo Alto Networks, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

² Lihat <https://www.bsa.org/policy-filings/indonesia-usabc-bsa-comments-on-draft-indonesia-personal-data-protection-bill>

³ Lihat <https://www.bsa.org/policy-filings/indonesia-bsa-joint-submission-on-gr82-amendment-matrix>

memungkinkan pemangku kepentingan industri untuk memberikan *feedback* terperinci mengenai rekomendasi-rekomendasi spesifik, yang mengarah pada keterlibatan komprehensif yang dapat membantu KOMINFO dengan lebih baik saat merevisi peraturan tersebut untuk mencapai tujuan-tujuan dari peraturan. Selain itu, mengomunikasikan dengan jelas tentang jadwal dan pencapaian untuk proses konsultasi publik akan membantu para pemangku kepentingan dalam memahami kapan Peraturan PDP akan diterbitkan dan jangka waktu yang diharapkan untuk implementasi selanjutnya. Kejelasan tersebut akan berkontribusi pada proses yang berkenaan dengan pengaturan yang efisien dan transparan di mana pemangku kepentingan dapat memberikan *feedback* yang lebih berarti kepada KOMINFO.

BSA menghargai kesempatan untuk memberikan komentar awal kami tentang Rancangan Peraturan PDP. Namun, karena terbatasnya waktu yang tersedia, komentar kami difokuskan pada kekhawatiran-kekhawatiran yang paling mendesak. Dengan tinjauan yang lebih menyeluruh terhadap Rancangan Peraturan PDP, terdapat kemungkinan bahwa kekhawatiran tambahan akan muncul. Oleh karena itu, kami dengan hormat meminta kesempatan untuk terlibat dalam diskusi lebih lanjut dan memberikan komentar yang lebih komprehensif di luar batas waktu 14 September 2023. Dialog yang diperpanjang akan memungkinkan kami untuk berkontribusi lebih penuh dalam pengembangan Rancangan Peraturan PDP.

Duplikasi antara UU PDP dengan Rancangan Peraturan PDP

Efisiensi dan kejelasan Rancangan Peraturan PDP dapat ditingkatkan dengan, jika memungkinkan, meminimalkan duplikasi antara Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (**UU PDP**) dengan Rancangan Peraturan PDP. Beberapa ketentuan dalam Rancangan Peraturan PDP mengulangi, baik dalam istilah yang sama atau sedikit berbeda, ketentuan-ketentuan UU PDP. Berikut ini adalah daftar *non-exhaustive* dari pengulangan tersebut:

- Pasal 1 Rancangan Peraturan PDP dan UU PDP sama-sama memuat definisi; di mana definisi-definisi tersebut identik, seharusnya dihapus dari Peraturan. Dalam hal terdapat definisi yang berbeda, para pihak dapat menjadi bingung tentang definisi mana yang berlaku;
- Pasal 2 Rancangan Peraturan PDP dan UU PDP keduanya mengatur aplikasi dan ruang lingkup dokumen masing-masing;
- Pasal 5 Rancangan Peraturan PDP secara efektif memperluas definisi Data Pribadi;
- Pasal 6 Rancangan Peraturan PDP dan Pasal 4 UU PDP keduanya mengatur perbedaan antara Data Pribadi "spesifik" dan "umum"; dan
- Pasal 9 Rancangan Peraturan PDP dan Pasal 16 UU keduanya mengatur definisi "Pengolahan".

BSA akan sangat menyambut baik kesempatan untuk bertemu KOMINFO untuk membahas duplikasi ini, dan duplikasi lainnya, dan bagaimana struktur Rancangan Peraturan PDP dapat dioptimalkan untuk mempromosikan kejelasan dan kepastian bagi para pemangku kepentingan.

Ekstrateritorialitas

Pasal 2(1)(b) Rancangan Peraturan PDP menyatakan bahwa peraturan tersebut mengatur mengenai "Setiap Orang, Badan Publik, dan Organisasi Internasional yang melakukan Pemrosesan Data Pribadi di luar wilayah hukum Republik Indonesia, yang memiliki konsekuensi hukum dalam wilayah hukum Republik Indonesia; dan/atau terhadap Subjek Data Pribadi warga negara Indonesia di luar wilayah hukum Republik Indonesia." Pasal 2(1)(b) tidak mendefinisikan yang dimaksud dengan "akibat atau konsekuensi hukum" dalam konteks penerapan dalam yurisdiksi Indonesia dan warga negara Indonesia di luar Indonesia. BSA merekomendasikan penyederhanaan penerapan ekstrateritorial yang dipertimbangkan dalam UU PDP, khususnya untuk memasukkan ke dalam Rancangan Peraturan PDP

mengenai definisi "akibat atau konsekuensi hukum" yang dibatasi pada penyediaan barang dan jasa oleh siapa pun di luar Indonesia, dengan maksud menargetkan individu di Indonesia atau juga menargetkan orang Indonesia yang berbasis di luar negeri.

Peran dan tanggung jawab Pengendali Data dan Prosesor Data

BSA menghargai pengenalan konsep Pengendali Data Pribadi dan Prosesor Data Pribadi dalam Undang-Undang Perlindungan Data Pribadi dan Rancangan Peraturan PDP yang selaras dengan banyak peraturan privasi di seluruh dunia. Kami merekomendasikan penyempurnaan lebih lanjut dari peran dan tanggung jawab yang diberikan kepada Pengendali Data Pribadi dan Prosesor Data Pribadi, termasuk:

- Pasal 20 mengakui bahwa Pengendali Data Pribadi dapat menunjuk Prosesor Data Pribadi. Berdasarkan Pasal 20(2), Prosesor Data Pribadi diharuskan untuk memproses data "berdasarkan instruksi Pengendali Data Pribadi". Namun, Pasal 213 tampaknya mempertimbangkan pengenaan sanksi administratif pada Prosesor Data Pribadi selain Pengendali Data Pribadi. Mengingat bahwa Prosesor Data Pribadi diharuskan untuk memproses data sesuai dengan instruksi pengendali, dan pengendali diharuskan untuk menentukan tujuan dan kontrol pemrosesan, BSA merekomendasikan untuk mengubah Rancangan Peraturan PDP sehingga Prosesor Data Pribadi tidak dikenakan sanksi ketika mereka bertindak berdasarkan instruksi Pengendali Data Pribadi.
- Pasal 156(1)-(2) mengatur bahwa Prosesor Data Pribadi wajib memastikan keakuratan Data Pribadi, termasuk melakukan verifikasi data. Namun, Prosesor Data Pribadi biasanya tidak memiliki hubungan langsung dengan Subjek Data Pribadi dan seringkali tidak memiliki akses ke data yang mereka simpan atas nama Pengendali Data Pribadi, sehingga sulit bagi mereka untuk secara langsung memastikan keakuratan data pribadi. Dalam beberapa kasus, Prosesor Data Pribadi bahkan mungkin secara kontrak dilarang melihat atau mengakses data yang mereka proses atas nama Pengendali Data Pribadi, dan oleh karena itu, tidak akan dapat memastikan keakuratan data pribadi tersebut. Kami merekomendasikan untuk menghapus ketentuan ini.
- Pasal 192 dan 194 mewajibkan baik Pengendali Data Pribadi dan Prosesor Data Pribadi untuk mencatat dan memetakan transfer data pribadi ke luar Indonesia, yang pada dasarnya melakukan penilaian dampak transfer data. Kami menyarankan untuk merevisi ketentuan ini agar hanya mewajibkan satu entitas untuk melakukan penilaian tersebut, untuk menghindari pengulangan ketika Prosesor Data Pribadi bertindak atas instruksi Pengendali Data Pribadi. Dalam skenario tersebut, Pengendali Data Pribadi cukup melakukan penilaian dampak transfer data.
- Pasal 195 mewajibkan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi untuk memberikan informasi kepada Subjek Data Pribadi sebelum transfer data pribadi. Sekali lagi, kami merekomendasikan untuk mengubah Rancangan Peraturan PDP sedemikian rupa agar membuat Pengendali Data Pribadi bertanggung jawab untuk melakukannya karena Pengendali Data Pribadi umumnya adalah entitas yang memiliki hubungan langsung dengan Subjek Data Pribadi.

Singkatnya, BSA merekomendasikan agar Pasal 156 (1) - (2), 192, 194 dan 195 hanya mengharuskan Pengendali Data Pribadi untuk bertanggung jawab atas kewajiban di dalamnya, karena Pengendali Data Pribadi adalah pihak yang tepat untuk mengambil kewajiban tersebut. Untuk wawasan lebih lanjut tentang bagaimana peran dan tanggung jawab pengontrol data dan pemroses data seharusnya

dibedakan, dapat dilihat dalam makalah BSA berjudul “*The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation.*”⁴

Persetujuan dan dasar tambahan untuk pemrosesan

UU PDP menciptakan enam dasar hukum bagi perusahaan untuk memproses data pribadi. Kami merekomendasikan tiga perubahan pada perlakuan Rancangan Peraturan PDP terhadap basis-basis pemrosesan ini.

Pertama, Pasal 14(d) mensyaratkan bahwa Pengendali Data Pribadi harus membatasi pengungkapan data pribadi untuk tujuan yang telah disetujui oleh Subjek Data Pribadi. Persyaratan ini dapat mengganggu pemrosesan yang dilakukan berdasarkan dasar hukum lainnya, termasuk pemenuhan kewajiban perjanjian dengan Subjek Data Pribadi, pemenuhan kewajiban hukum Pengendali Data Pribadi, antara lain, sebagaimana yang telah diatur dalam Pasal 20 UU PDP. BSA menyarankan untuk mengubah Pasal 14(d) sehingga Subjek Data Pribadi harus menyetujui pengungkapan data pribadi hanya jika persetujuan subjek data merupakan dasar hukum untuk pemrosesan.

Kedua, Pasal 54(5) menyatakan bahwa perjanjian kontraktual tidak dapat dianggap menggantikan posisi persetujuan sebagai dasar hukum untuk pemrosesan, dan Pasal 54(6) menyatakan bahwa Pengendali Data Pribadi tetap berkewajiban untuk menggunakan persetujuan sebagai dasar hukum pemrosesan untuk melakukan aktivitas pemrosesan yang memerlukan persetujuan. Pasal 55 (1) Rancangan Peraturan PDP menetapkan kewajiban tambahan ketika perusahaan bergantung kepada perjanjian, yaitu, pemenuhan kewajiban kontraktual, sebagai dasar untuk memproses data pribadi berdasarkan UU PDP. Berdasarkan Rancangan Peraturan PDP, meskipun perusahaan bergantung pada perjanjian, hal tersebut tetap membutuhkan persetujuan yang eksplisit dan sah dari Subjek Data Pribadi. Ketiga Pasal tersebut bertentangan dengan posisi UU PDP yang mengakui kebutuhan kontraktual sebagai dasar independen untuk memproses data pribadi. Hal ini menciptakan kebingungan dan ambiguitas bagi bisnis dan konsumen.

BSA menyarankan untuk merevisi ketentuan-ketentuan tersebut untuk menghindari mewajibkan perusahaan untuk mendapatkan persetujuan tambahan untuk memproses data, ketika mereka sudah memproses data tersebut berdasarkan alasan lain untuk pemrosesan yang diakui dalam Pasal 20 UU PDP. Seperti tertulis, Rancangan Peraturan PDP terlalu bergantung pada persetujuan, dan akan mengakibatkan subjek data individu menerima berbagai permintaan persetujuan bahkan ketika perusahaan memproses data mereka sesuai dengan perjanjian terpisah yang ada. Hasil ini bertentangan dengan UU PDP, yang mengakui persetujuan dan kebutuhan kontraktual sebagai dasar independen untuk memproses data pribadi. Oleh karena itu, kami sarankan untuk menghapus Pasal 54(5)-(6) dan 55(1)(a).

Ketiga, Pasal 71 mewajibkan Pengendali Data Pribadi untuk mendokumentasikan dan menyerahkan hasil analisis dan penilaian kepentingan yang sah kepada Subjek Data Pribadi. Persyaratan ini melampaui undang-undang perlindungan data global lainnya, yang mengharuskan perusahaan untuk melakukan analisis penerapan dasar kepentingan yang sah untuk pemrosesan — namun tidak mewajibkan analisis tersebut diberikan kepada Subjek Data Pribadi individu. Mengirimkan analisis ke Subjek Data Pribadi dapat menciptakan risiko privasi atau keamanan baru, seperti ketika perusahaan mengandalkan kepentingan yang sah untuk memproses data untuk tujuan seperti deteksi penipuan atau keamanan siber, di mana pengungkapan proaktif seputar jenis proses ini pada akhirnya dapat merusak efektivitasnya. Oleh karena itu, BSA merekomendasikan untuk menghapus Pasal 71.

Kegagalan Perlindungan Data Pribadi

Pasal 124 hingga 126 Rancangan Peraturan PDP mengatur mengenai persyaratan Pengendali Data Pribadi untuk memberitahukan kepada pemangku kepentingan tentang kegagalan Perlindungan Data Pribadi. Rancangan Peraturan PDP tidak mengatur mengenai definisi "kegagalan Perlindungan Data Pribadi" tersebut. Untuk kejelasan, BSA merekomendasikan untuk memasukkan definisi yang mirip dengan bagaimana pelanggaran data didefinisikan di yurisdiksi lain. Sebagai contoh, *European General Data Protection Regulation (GDPR)* mendefinisikan "pelanggaran data pribadi" sebagai pelanggaran keamanan yang mengarah pada penghancuran, kehilangan, perubahan, pengungkapan

⁴ Lihat <https://www.bsa.org/policy-filings/the-global-standard-distinguishing-between-controllers-and-processors-in-privacy-legislation>

yang tidak sah, atau akses ke, data pribadi yang dikirim, disimpan, atau diproses secara tidak sengaja atau melanggar hukum, sementara *Singapore Personal Data Protection Act (PDPA)* mendefinisikan "pelanggaran data" sehubungan dengan data pribadi sebagai akses, pengumpulan, penggunaan, pengungkapan, penyalinan, modifikasi, atau pembuangan data pribadi yang tidak sah; atau hilangnya media penyimpanan atau perangkat tempat data pribadi disimpan dalam keadaan di mana akses, pengumpulan, penggunaan, pengungkapan, penyalinan, modifikasi, atau pembuangan data pribadi yang tidak sah mungkin terjadi.

Berdasarkan Pasal 124, Pengendali Data akan diminta untuk melaporkan pelanggaran kepada Lembaga PDP dan kepada Subjek Data Pribadi individu dalam waktu tiga hari — bahkan ketika pelanggaran tersebut tidak menciptakan risiko bahaya yang signifikan, sehingga menambah kompleksitas yang tidak perlu pada proses. Karena itu, kami menawarkan hal-hal berikut untuk dipertimbangkan.

Pemberitahuan Kegagalan Perlindungan Data Pribadi kepada Lembaga PDP

Rancangan Peraturan PDP mensyaratkan pelanggaran data pribadi untuk dilaporkan ke Lembaga PDP, termasuk pelanggaran data pribadi yang berisiko rendah kepada Subjek Data Pribadi. Hal ini dapat mengakibatkan kelelahan notifikasi baik bagi Lembaga PDP maupun pengontrol data, yang mengikis efektivitas persyaratan notifikasi. BSA merekomendasikan bahwa ambang batas pemberitahuan kepada Lembaga PDP adalah perolehan data pribadi yang tidak terenkripsi atau tidak disunting secara tidak sah yang menciptakan risiko bahaya material bagi Subjek Data Pribadi sehingga Lembaga PDP dan pengontrol data dapat memfokuskan upaya mereka dengan tepat pada pelanggaran tersebut.

Pemberitahuan Kegagalan Perlindungan Data Pribadi kepada Subjek Data Pribadi

Pemberitahuan setiap pelanggaran data kepada Subjek Data Pribadi terlepas dari seberapa signifikannya, adalah kontraproduktif. Praktik semacam itu dapat menyebabkan alarm yang tidak perlu dalam kasus pelanggaran data yang tidak penting, atau kelelahan pemberitahuan di antara Subjek Data Pribadi di mana mereka gagal mengambil langkah-langkah yang diperlukan untuk melindungi data pribadi mereka sendiri bahkan dalam kasus-kasus serius. Oleh karena itu, BSA merekomendasikan persyaratan pemberitahuan yang lebih selektif, di mana pemberitahuan diperlukan hanya ketika ada dampak negatif yang signifikan pada Subjek Data Pribadi.

Timeline Pemberitahuan kepada Lembaga PDP dan Subjek Data Pribadi

Meskipun kami mendukung pemberitahuan segera tentang pelanggaran yang menciptakan risiko signifikan kerugian material bagi individu, kami sangat menyarankan untuk meninjau kembali persyaratan untuk tenggang waktu 3 x 24 jam yang ketat untuk pemberitahuan. Mematuhi *timeline* yang ketat seperti itu dapat mengalihkan sumber daya yang berharga ke arah upaya pelaporan dan komunikasi alih-alih berfokus pada memperbaiki pelanggaran data. Oleh karena itu, kami mengusulkan kerangka waktu yang lebih fleksibel yang memungkinkan pengontrol data untuk mengelola pelanggaran dan proses pemberitahuan secara efektif. Secara khusus, kami merekomendasikan agar batas waktu 3 x 24 jam untuk memberi tahu Subjek Data Pribadi dan lembaga PDP diubah menjadi pemberitahuan yang dibuat "tanpa penundaan yang tidak semestinya."

Transfer Data Lintas Batas

Rancangan Peraturan PDP juga menerapkan pembatasan UU PDP tentang transfer data lintas batas. Kami merekomendasikan tiga revisi untuk aspek peraturan ini:

- Pertama, Pasal 185(2) Rancangan Peraturan PDP menetapkan mekanisme transfer data pribadi lintas batas untuk memastikan "Perlindungan Data Pribadi yang memadai dan mengikat." BSA mengusulkan untuk memasukkan sertifikasi sebagai mekanisme yang valid untuk menciptakan lebih banyak fleksibilitas dalam mendukung transfer data lintas batas. Sertifikasi yang diakui secara internasional seperti ISO 27701, Global and APEC Cross Border Privacy Rules (**CBPR**) dan sertifikasi lain semacam itu harus diakui untuk memungkinkan transfer data pribadi di luar Indonesia. Sertifikasi ini telah terbukti bermanfaat bagi perusahaan yang beroperasi melintasi batas-batas nasional dalam menunjukkan kepatuhan mereka terhadap standar privasi data yang dapat dioperasikan secara global dan dapat dipercaya.

- Kedua, Pasal 187 memungkinkan Lembaga PDP untuk menentukan klausul kontrak standar. BSA merekomendasikan agar Lembaga PDP mempertimbangkan untuk mengakui klausul kontrak standar lain yang diterima secara luas, seperti *EU Standard Contractual Clauses (SCC)* dan *ASEAN Model Contractual Clauses (MCC)*. Menyetujui penggunaan klausul kontrak standar yang diakui di yurisdiksi lain akan memungkinkan Pengendali Data Pribadi untuk melayani pelanggan di Indonesia dengan menggunakan kontrak yang ada yang menciptakan kewajiban perlindungan data yang kuat dan selaras dengan praktik internasional yang telah ditetapkan. BSA lebih lanjut merekomendasikan agar Lembaga PDP melakukan konsultasi publik untuk mengumpulkan komentar industri sebelum merilis klausul kontrak standar yang disetujui.
- Terakhir, Pasal 188(3) mewajibkan Pengendali Data Pribadi untuk mendapatkan persetujuan dari Lembaga PDP sebelum mentransfer data pribadi saat menggunakan aturan perusahaan yang mengikat (**APM**) sebagai mekanisme transfer data lintas batas. Kami merekomendasikan Lembaga PDP untuk mengakui bahwa APM yang telah menerima persetujuan dari otoritas perlindungan data lainnya dapat dianggap sebagai mekanisme transfer data yang dapat diterima berdasarkan UU PDP tanpa perlu mendapatkan persetujuan terpisah dari otoritas Indonesia.

Memungkinkan pengontrol data untuk menggunakan mekanisme yang berbeda untuk mentransfer data pribadi melintasi perbatasan internasional memberikan fleksibilitas kepada bisnis untuk menentukan mekanisme yang paling optimal dan relevan bagi mereka. Singkatnya, BSA merekomendasikan untuk mengenali lebih banyak mekanisme untuk transfer data pribadi lintas batas, termasuk sertifikasi, klausul kontrak standar dari wilayah lain, dan APM yang disetujui di yurisdiksi lain.

Menanggapi Permintaan Subjek Data

Pasal 84, 89, 90, dan 99 mewajibkan Pengendali Data Pribadi untuk menanggapi permintaan Subjek Data Pribadi sehubungan dengan mengoreksi, memberikan akses, memberikan salinan, dan menghapus data pribadi dalam jangka waktu selambat-lambatnya 3 x 24 jam. Ini adalah jangka waktu yang tidak memadai bagi Pengendali Data Pribadi untuk menanggapi permintaan Subjek Data Pribadi secara memadai, yang dapat bervariasi secara signifikan dalam volume dan cakupan. BSA merekomendasikan agar jangka waktu di mana Pengendali Data Pribadi diharuskan untuk mematuhi permintaan Subjek Data Pribadi harus direvisi agar sejalan dengan praktik di yurisdiksi lain. Misalnya, GDPR mewajibkan pengontrol data untuk menanggapi permintaan hak konsumen tanpa penundaan yang tidak semestinya dan dalam waktu satu bulan sejak permintaan, dengan opsi untuk memperpanjang batas waktu dua bulan lagi, dan opsi bagi pengontrol data untuk membebaskan biaya yang wajar atau menolak untuk mengabaikan permintaan dalam beberapa kasus.⁵ PDPA Singapura mewajibkan organisasi untuk menanggapi permintaan Subjek Data Pribadi sesegera mungkin, dalam waktu 30 hari.⁶ BSA merekomendasikan untuk mewajibkan Pengendali Data Pribadi untuk menanggapi permintaan Subjek Data Pribadi tanpa penundaan yang tidak semestinya dan dalam waktu 30 hari, dengan opsi untuk memperpanjang batas waktu dua bulan lagi dengan memberitahukan kepada Subjek Data Pribadi, dan menolak untuk mengabaikan permintaan dalam kasus di mana permintaan tersebut tidak berdasar atau berlebihan.

Mekanisme kompensasi

Ketentuan-ketentuan dalam Pasal 117-120 mewajibkan Pengendali Data Pribadi untuk mengatur dan menerapkan mekanisme, kebijakan, dan proses kompensasi di mana Subjek Data Pribadi dapat mengklaim dan menerima jumlah kompensasi yang relevan secara langsung dari Pengendali Data Pribadi, setelah menyerahkan bukti kerugian nominal atau non-material untuk setiap kegagalan perlindungan data pribadi. Ketentuan ini berisiko membuka serentetan pengajuan yang tidak berdasar, yang akan menambah beban dan biaya yang tidak perlu bagi Pengendali Data Pribadi. Selanjutnya,

⁵ Lihat Pasal 12 EU GDPR di <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>

⁶Lihat Bagian 21 (1) *Singapore PDPA* di <https://sso.agc.gov.sg/Act/PDPA2012>, dan *Personal Data Protection Regulations 2021*, Bagian 2 di <https://sso.agc.gov.sg/SL/PDPA2012-S63-2021>.

Pasal 117(a) menyatakan bahwa Subjek Data Pribadi wajib menyerahkan bukti pelanggaran pemrosesan Data Pribadi yang berdampak pada Subjek Data Pribadi, tanpa harus membuktikan kerugian yang diderita oleh Subjek Data Pribadi tersebut. BSA merekomendasikan bahwa setiap klaim kompensasi harus didasarkan pada arahan, atau diarahkan kepada, otoritas perlindungan data yang relevan, yaitu, Lembaga PDP. Tanpa panduan yang tepat dan preseden yang relevan, ketentuan tersebut dapat mengakibatkan ketidakpastian hukum yang cukup besar. Kami selanjutnya merekomendasikan untuk menyertakan persyaratan bagi Subjek Data Pribadi untuk membuktikan bahwa pelanggaran tersebut menyebabkan bahaya yang sebenarnya. Terakhir, BSA merekomendasikan untuk menghapus frasa "tanpa harus membuktikan kerugian yang diderita oleh Subjek Data Pribadi" dalam Pasal 117 (a).

Kesimpulan

Dalam konteks *Digital Economy Framework Agreement (DEFA)* yang diinisiasi oleh ASEAN, sangat penting bagi Indonesia untuk memprioritaskan keselarasan kerangka regulasi dengan tujuan regional. Untuk mempromosikan kerja sama yang mulus dan mendorong pertumbuhan ekonomi digital, kami merekomendasikan agar Indonesia menilai dengan cermat Rancangan Peraturan PDP sebagaimana mestinya.

BSA menghargai kesempatan untuk memberikan komentar dan rekomendasi kami tentang Rancangan Peraturan PDP. Kami berharap komentar kami akan membantu dalam pengembangan peraturan yang jelas dan ketat untuk perlindungan data pribadi di Indonesia. Kami berharap dapat melanjutkan keterlibatan kami dengan KOMINFO dan instansi terkait mengenai perlindungan data pribadi dan kebijakan privasi dan meminta agar KOMINFO mempertimbangkan pengiriman terperinci lebih lanjut melewati batas waktu yang ditentukan pada 14 September 2023. Kami mendorong KOMINFO untuk terus melibatkan sektor swasta tentang bagaimana untuk lebih meningkatkan Rancangan Peraturan PDP. **Kami ingin mengambil kesempatan ini untuk mengusulkan pertemuan dengan Bapak dan Ibu untuk membahas Rancangan Peraturan PDP lebih lanjut, sesuai dengan ketersediaan waktu dari Bapak dan Ibu.** Jangan ragu untuk menghubungi yang bertandatangan di bawah ini melalui email waisanw@bsa.org untuk melanjutkan diskusi.

Hormat kami,

Wong Wai San

Wong Wai San

Senior Manager, Policy – APAC