Asosiasi Media Siber Indonesia

ICT watch! ictwatch.id

Didukung oleh:

ABC INTERNATIONAL DEVELOPMENT

Laporan Penilaian Kepatuhan Pelindungan Data Pribadi untuk Perusahaan Media

Daftar Isi

*****

Laporan Penilaian Kepatuhan Pelindungan Data Pribadi untuk Perusahaan Media

Penulis : 1. Bhredipta Socarana, S.H., LLM.,CIPP/E

2. Rahma Atika Idrus, S.H.

3. Archandra Viryasatya Sugama, S.IP

Penyusun : 1. Bhredipta Socarana, S.H., LLM.,CIPP/E

2. Rahma Atika Idrus, S.H.

3. Archandra Viryasatya Sugama, S.IP

Perancang sampul : Bhredipta Socarana, S.H., LLM.,CIPP/E

Tata Letak : Archandra Viryasatya Sugama, S.IP

Diterbitkan oleh :

Asosiasi Media Siber Indonesia

Asosiasi Media Siber Indonesia (AMSI)

Gedung Tempo Media

Jl. Palmerah Barat No. 8, Jakarta Selatan 12210

Website: www.amsi.or.id

Email: info@amsi.or.id

Edisi Pertama : Mei 2024

Indonesia Media Program dilaksanakan oleh ABC International Development dan didanai oleh Pemerintah Australia berdasarkan Strategi Penyiaran Indo-Pasifik.

1. Latar Belakang

Di dalam negara demokrasi, pers dan media memiliki peran penting dalam meningkatkan partisipasi publik serta mewujudkan kebebasan berpendapat. Dalam menjalankan fungsinya, Perusahaan Pers tidak terlepas dari kegiatan pemrosesan data pribadi, baik data pribadi karyawan, konsumen, maupun pihak lain. Pemrosesan data pribadi ini dilakukan baik dalam konteks kegiatan jurnalisme, operasional, maupun komersial dari Perusahaan Pers.

Di Indonesia, kegiatan pers diatur oleh UU No. 40 Tahun 1999 tentang Pers serta Kode Etik Jurnalistik, yang juga mengatur hak-hak privasi narasumber, hak untuk menutupi identitas narasumber hingga larangan identitas anak-anak secara jelas, baik nama anak-anak tersebut sebagai pelaku, atau diduga sebagai pelaku kejahatan. Selain itu, UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (**UU PDP**) yang disahkan pada tahun 2022 dan sepenuhnya dilaksanakan pada bulan Oktober 2024 juga turut berlaku kepada seluruh Perusahaan Pers. Pelanggaran terhadap ketentuan pelindungan data pribadi dapat dikenakan sanksi administratif, pidana, hingga gugatan oleh pihak terkait jika menimbulkan kerugian. Oleh karena itu, upaya untuk mewujudkan kepatuhan Perusahaan Pers terhadap regulasi dan peraturan terkait data pribadi menjadi sangat penting.

Selain kebutuhan untuk mematuhi regulasi dan peraturan yang berlaku, terdapat berbagai bentuk kejahatan yang menyasar pada data pribadi, dimulai dari serangan siber, *phishing, malware*, dan *social engineering* (Forbes, 2022). Studi dari Stanford University dan Tessian (2020) menemukan bahwa 88% kebocoran data diakibatkan oleh kelalaian manusia yang dapat disalahgunakan untuk aktivitas yang merugikan seperti pinjaman *online* ilegal, pembobolan rekening, hingga peretasan (*hacking)*.

Tidak hanya itu, kewaspadaan masyarakat terhadap pentingnya data pribadi juga meningkat. Di Amerika Serikat misalnya, studi dari Pew Research Center (2023) menunjukkan bahwa 71 persen penduduk dewasa merasa khawatir tentang bagaimana data mereka dipergunakan oleh pemerintah sedangkan 81 persen khawatir tentang bagaimana perusahaan menggunakan data mereka. Di Indonesia, survei Kementerian Komunikasi dan Informatika dan Katadata Insight Center (2021) menemukan pemahaman masyarakat terkait data pribadi umum berada di tingkat sedang sedangkan implementasinya tergolong kurang.

Laporan ini yang merupakan kerja sama antara ICT Watch dan Asosiasi Siber Media Indonesia (AMSI) disusun untuk mengetahui posisi anggota AMSI sebagai Perusahaan Pers yang bergerak di aktivitas jurnalisme (**Perusahaan Pers**) dalam kesiapan untuk mematuhi ketentuan UU PDP ketika melakukan pemrosesan data pribadi. Melalui *assessment* ini, dapat ditemukan capaian, tantangan, dan potensi perbaikan dalam kebijakan serta praktik pengelolaan data pribadi oleh Perusahaan Pers. Hal ini selaras dengan visi dan misi AMSI untuk membangun ekosistem media siber Indonesia yang sehat, demokratis, berkualitas, jurnalisme yang bertanggung jawab, patuh pada kode etik, dan tunduk pada kepentingan umum serta adaptif terhadap perkembangan teknologi.

Dengan demikian, laporan ini diharapkan dapat memberikan gambaran komprehensif terkait kesiapan implementasi UU PDP di lingkungan AMSI, serta mendorong upaya peningkatan pelindungan data pribadi di lingkungan industri pers.

2. Metodologi dan Batasan

Sesuai kebutuhan AMSI, laporan ini disusun untuk menunjukan kondisi kesiapan dan implementasi pelindungan data pribadi Perusahaan Pers yang merupakan anggota AMSI. Analisis yang tersedia dalam laporan ini berasal dari informasi dan data yang dikumpulkan dari anggota AMSI melalui kuesioner berisi pertanyaan seputar aktivitas kegiatan pemrosesan data pribadi. Untuk mendapatkan gambaran utuh, analisis perlu dilakukan kepada informasi

dan data yang bersumber dari seluruh anggota AMSI. Namun dikarenakan keterbatasan sumber daya dan waktu, beberapa penyesuaian dilakukan sebagai berikut:

a. Informasi dan data yang dikumpulkan secara komprehensif dilakukan terhadap lima Perusahaan Pers yang merupakan anggota AMSI. Kelima media tersebut dipilih oleh AMSI berdasarkan estimasi kegiatan operasionalnya yang secara aktif melakukan pemrosesan data pribadi. Pengumpulan data dan informasi meliputi reviu dokumen, uji coba pada situs, serta penelusuran di internet mengenai praktik pelindungan data pribadi kelima media tersebut. Kuesioner yang dibagikan kepada lima media tersebut berisi pertanyaan yang bersifat terbuka (*open-ended*), terkait kegiatan pelindungan data pribadi kelima media.

b. Informasi dan data dilakukan secara terbatas terhadap 50 Perusahaan Pers[1] anggota AMSI. Pengumpulan data dilakukan terbatas hanya melalui informasi yang diterima berdasarkan jawaban pada kuesioner. Kuesioner yang diberikan disusun dengan pertanyaan dan pilihan jawaban terbatas (ya/tidak/tidak tahu) untuk mengoptimalkan ketersediaan sumber yang terbatas dalam melakukan analisis.

c. Baseline information yang berasal dari informasi bersumber pada poin (a) akan menjadi dasar penyusunan *gap assessment* dan *checklist recommendation* sebagai keluaran dari laporan ini. Terhadap informasi yang bersumber dari poin (b) akan dilakukan *gap assessment* terbatas terhadap keluaran dari poin (a). Penyesuaian terbatas akan dilakukan terhadap *checklist recommendation* berupa informasi yang memberikan konteks perbedaan kondisi antara lima perusahaan pada poin (a) dan perusahaan pada poin (b) sehingga ketika perusahaan pada poin (b) mencapai kondisi seperti perusahaan pada poin (a) dapat menyesuaikan praktik pelindungan data pribadinya.

3. Sistematika Penulisan

Laporan ini terdiri atas 10 bagian utama meliputi, (1) Latar Belakang, (2) Metodologi dan Batasan, (3) Sistematika Penulisan, (4) Kualifikasi, (5) Analisis Keberlakuan UU PDP Bagi Perusahaan Pers, (6) *Baseline Information* yang akan terdiri atas informasi terkait lima perusahaan pers sampel dan risalah singkat 50 Perusahaan Pers anggota AMSI, (7) Gap Assessment berdasarkan informasi yang diterima dari lima perusahaan pers sampel, konteks terbatas dari 50 Perusahaan Pers anggota AMSI, serta langkah teknis tindak lanjut yang diperlukan untuk mencapai kondisi ideal, (8) kesimpulan dan rekomendasi, (9) penutup, serta (10) lampiran.

Turut disertakan pada laporan ini lampiran berupa C*ompliance Checklist* Kepatuhan Pelindungan Data Pribadi bagi anggota AMSI.

4. Kualifikasi

a. Dokumen ini merupakan dokumen yang bersifat panduan, tidak mengikat secara hukum, dan hanya memberikan penjelasan langkah – langkah praktis tata kelola pelindungan data pribadi. Dokumen ini bukan merupakan suatu nasihat hukum sehingga pemanfaatan dan penggunaannya tidak menjadi tanggung jawab penyusun.

[1] Informasi Penulis: Pada versi laporan 1 April 2024, tertulis 53 Perusahaan Pers sebagai responden kuesioner. Namun setelah dilakukan penelusuran terdapat 5 respon yang diterima dari Perusahaan Pers sampel (Tribunnews, Tempo, Dari Laut, Batam News, dan Berita Jatim). Untuk memastikan analisis antara Perusahaan Pers Sampel dan 50 Perusahaan Pers berbeda, respon dari Perusahaan Dari Laut, Batam News, dan Berita Jatim tidak disertakan karena sumber pengisian sama dengan yang diterima pada kuesioner Perusahaan Pers. Sedangkan untuk Tribunnews dan Tempo tetap dianalisis sebagai bagian dari 50 Perusahaan Pers karena sumber informasi berbeda dari yang diterima pada kuesioner Perusahaan Pers sampel.

b. Dokumen ini disusun berdasarkan analisis terhadap kebutuhan pemenuhan kewajiban pelindungan data pribadi yang dikumpulkan dari lima perusahaan pers anggota AMSI. Analisis dan informasi terbatas juga ditambahkan sesuai hasil kuesioner dari 50 Perusahaan Pers anggota AMSI.

c. Khusus untuk *checklist compliance*, dokumen tersebut disusun berdasarkan informasi yang didapat dari lima Perusahaan Pers sampel anggota AMSI. Pemakaian oleh pihak selain lima Perusahaan Pers anggota AMSI membutuhkan penyesuaian yang mungkin saja belum terakomodasi dalam dokumen *checklist compliance*, kecuali dijelaskan lain.

d. Dokumen ini disusun dengan merujuk peraturan perundang – undangan terkait, praktik industri serta rancangan peraturan perundang – undangan. Mengingat sifat rujukan rancangan peraturan perundang – undangan dapat berubah, maka pengguna dokumen ini perlu memastikan kesesuaian dan keterbaruan informasi yang berlaku dalam dokumen ini.

e. Analisis ini dilakukan berdasarkan respon yang diterima pada kuesioner, reviu terhadap situs dan platform Perusahaan Pers, serta reviu terhadap dokumen Perusahaan Pers. Kelima Perusahaan Pers yang direviu merupakan Perusahaan Pers yang mengoperasikan platform dan/atau situs untuk menampilkan karya jurnalistiknya kepada konsumen, memproses data pribadi pembaca baik melalui pendaftaran berlangganan atau melalui fitur widget iklan, serta memiliki karyawan dan vendor dalam pengoperasiannya. Reviu juga kami lakukan dengan menggunakan akses internet dari luar wilayah Indonesia.

f. Dikarenakan keterbatasan sumber daya, tidak dilakukan analisis terhadap dokumen, platform, sistem internal dan/atau situs 50 Perusahaan Pers anggota AMSI, sehingga analisis hanya dilakukan terhadap informasi yang diterima melalui kuesioner.

5. Analisis Keberlakuan UU PDP Bagi Perusahaan Pers

5.1. Keberlakuan UU PDP terhadap Perusahaan Pers

UU PDP berlaku kepada setiap orang, badan publik, dan organisasi internasional yang melakukan perbuatan hukum yang diatur pada UU PDP, termasuk kegiatan pemrosesan data pribadi,[2] apabila, kegiatan tersebut (1) terjadi di wilayah hukum Negara Republik Indonesia; dan (2) di luar wilayah hukum Republik Indonesia namun memiliki akibat hukum di wilayah hukum Negara Republik Indonesia dan/atau kepada subjek data pribadi warga negara Indonesia di luar wilayah hukum Negara Republik Indonesia. Sepanjang suatu entitas melakukan kegiatan pemrosesan data pribadi warga negara Indonesia atau warga negara asing di Indonesia, maka UU PDP wajib untuk dipatuhi.

Perusahaan Pers wajib mematuhi UU PDP karena melakukan pemrosesan data pribadi, baik data pribadi spesifik maupun non-spesifik, yang berasal dari konsumen, karyawan, dan/atau penyedia jasa (vendor) Perusahaan Pers dengan beragam tujuan pemrosesan data pribadi.

UU PDP mengatur dalam setiap kegiatan pemrosesan terdapat pihak yang menentukan tujuan pemrosesan data pribadi dan melakukan kendali pemrosesan data pribadi (Pengendali), dan pihak yang melakukan pemrosesan data pribadi atas nama Pengendali (Prosesor). Perusahaan Pers, dapat menjadi Pengendali atau Prosesor dalam kegiatan data pribadi yang dilakukan. Meskipun mengingat model

[2] Pasal 16 UU PDP mengatur bahwa pemrosesan data pribadi meliputi kegiatan pemerolehan dan pengumpulan; pengolahan dan penganalisisan; penyimpanan; perbaikan dan pembaruan; penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/ atau, penghapusan atau pemusnahan.

bisnis dan kegiatan pemrosesan data pribadi yang dilakukan, Perusahaan Pers dapat lebih sering menjadi Pengendali.

UU PDP mengatur pengecualian terhadap keberlakuan UU PDP, jika pemrosesan Data Pribadi dilakukan oleh orang perseorangan dalam kegiatan pribadi atau rumah tangga. Meskipun UU PDP tidak menjelaskan definisi kegiatan rumah tangga, jika merujuk pada European Union General Data Protection Regulation (EU GDPR) kegiatan rumah tangga berarti kegiatan yang terkait urusan pribadi seseorang, dan tidak terkait kegiatan profesional maupun komersial.

Mengingat kegiatan pemrosesan data pribadi oleh Perusahaan Pers dilakukan dalam konteks komersial (untuk pemrosesan data pribadi konsumen), dan dalam konteks profesional (untuk pemrosesan data pribadi karyawan dan/atau vendor) maka pengecualian UU PDP tidak berlaku. Perusahaan Pers tetap wajib tunduk pada ketentuan UU PDP.

5.2. Kewajiban Perusahaan Pers Berdasarkan UU PDP

Ketentuan UU PDP mengatur kewajiban pengendali dan/atau prosesor dalam pemrosesan data pribadi yang dilakukannya. Namun, mengingat keterbatasan yang ada, dari daftar kewajiban yang terdapat pada UU PDP, dalam dokumen ini hanya akan dijelaskan, secara singkat,[3] kewajiban Perusahaan Pers sebagai pengendali, sebagai berikut:

1. Memiliki dasar pemrosesan Data Pribadi

UU PDP mewajibkan pengendali memiliki dasar pemrosesan data pribadi[4] yang sah dan sesuai untuk pemenuhan tujuannya. Dasar pemrosesan data pribadi menjadi legitimasi dan alas hak bagi pengendali dalam memproses data pribadi. Pemilihan dan penggunaan dasar pemrosesan data pribadi harus sesuai persyaratan peraturan perundang - undangan. Sebagai contoh, jika Pengendali memilih persetujuan subjek data sebagai dasar pemrosesan data pribadi, maka Pengendali wajib memberikan beberapa informasi[5] kepada subjek data pribadi, dan pada saat memproses data pribadi untuk menunjukkan bukti persetujuan yang telah diberikan oleh Subjek Data Pribadi.

2. Memproses Data Pribadi secara sesuai ketentuan peraturan perundangan

---

[3] Untuk detail kewajiban dapat merujuk pada ketentuan yang tercantum dalam UU PDP. Terkait teknis pelaksanaan dapat merujuk pada Compliance Checklist yang sudah disusun. Harap dicatat, Perusahaan Pers dapat menjadi subjek regulasi lain terkait pelindungan data pribadi yang belum terakomodasi dalam dokumen ini.

[4] Pasal 20 UU PDP mengatur bahwa dasar pemrosesan data pribadi meliputi (a) persetujuan yang sah secara eksplisit dari Subjek Data Pribadi untuk satu atau beberapa tujuan tertentu yang telah disampaikan oleh Pengendali Data Pribadi kepada Subjek Data Pribadi; (b) pemenuhan kewajiban perjanjian dalam hal Subjek Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Subjek Data Pribadi pada saat akan melakukan perjanjian; (c) pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;
(d) pemenuhan pelindungan kepentingan vital Subjek Data Pribadi; (e) pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengendali Data Pribadi berdasarkan peraturan perundang-undangan; dan/atau (f) pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan Pengendali Data Pribadi dan hak Subjek Data Pribadi

[5] Pasal 21 UU PDP mengatur informasi yang wajib disediakan meliputi, (a) legalitas dari pemrosesan Data Pribadi; (b) tujuan pemrosesan Data Pribadi; (c) jenis dan relevansi Data Pribadi yang akan diproses; (d) jangka waktu retensi dokumen yang memuat Data Pribadi; (e) rincian mengenai Informasi yang dikumpulkan; (f) jangka waktu pemrosesan Data Pribadi; dan (g) hak Subjek Data Pribadi.

UU PDP mewajibkan pengendali untuk memproses data pribadi secara terbatas dan spesifik,[6] sah secara hukum,[7] serta transparan.[8] Salah satu bentuk pemenuhan kewajiban tersebut adalah memastikan pengendali menggunakan dasar pemrosesan yang sesuai dan sah. Dalam pemrosesan data pribadi, pengendali hanya dapat memproses data pribadi sesuai tujuan pemrosesan data pribadi, dan harus memastikan akurasi kelengkapan, dan konsistensi data pribadi sesuai ketentuan yang berlaku. Selain itu, UU PDP mengatur dalam kondisi tertentu, pemrosesan data pribadi wajib diikuti dengan tindakan lain oleh pengendali. Contoh dari kewajiban ini adalah kewajiban pemberitahuan terkait pengalihan data pribadi kepada subjek data pribadi oleh pengendali yang berbadan hukum setelah dan sebelum terjadi penggabungan, pemisahan, pengambilalihan, peleburan, atau pembubaran badan hukum.

3. Memenuhi hak subjek data pribadi

Dalam relasi Pengendali dan subjek data pribadi, UU PDP mewajibkan Pengendali untuk memenuhi hak subjek data pribadi. Dari konteks pemenuhan hak, setidaknya terdapat tiga kondisi pemenuhan hak dalam UU PDP sebagai berikut:

a. Pemenuhan Hak Dalam Waktu Spesifik Tertentu

Dalam kondisi ini Pengendali wajib memenuhi permintaan subjek data pribadi sesuai waktu yang ditentukan oleh UU PDP. Sebagai contoh, UU PDP mengatur, dalam 3x24 jam setelah penerimaan permintaan subjek data pribadi untuk memperbarui dan/atau memperbaiki ketidakakuratan data pribadi, Pengendali harus memenuhi permintaan tersebut.

Ketentuan serupa berlaku untuk permintaan hak subjek data pribadi atas data pribadi yang diproses serta rekam jejak pemrosesan, penghentian pemrosesan data pribadi dalam hal subjek data menarik persetujuan, serta penundaan pemrosesan data pribadi.

Perlu dicatat, selain memenuhi waktu yang ditentukan, beberapa hak, seperti pembaruan dan/atau perbaikan data pribadi, dan hak pelaksanaan penundaan dan pembatasan pemrosesan data pribadi mensyaratkan pengendali memberitahukan hasil pelaksanaan permintaan subjek data pribadi. Selain pemenuhan hak, Pengendali juga wajib memberikan pemberitahuan tertulis kepada subjek data pribadi dan lembaga paling lambat 3x24 jam jika terjadi kegagalan pelindungan data pribadi.[9]

b. Pemenuhan Hak Tanpa Batas Waktu Spesifik

---

[6] UU PDP mengatur yang dimaksud dengan "secara terbatas dan spesifik adalah pengumpulan Data Pribadi harus terbatas sesuai dengan tujuan pemrosesannya serta tujuan pemrosesan Data Pribadi harus secara eksplisit, sah, dan telah ditentukan pada saat pengumpulan data pribadi.

[7] UU PDP mengatur yang dimaksud dengan "sah secara hukum" adalah pemrosesan Data Pribadi dilakukan sesuai dengan ketentuan peraturan perundang undangan.

[8] UU PDP mengatur yang dimaksud dengan "transparan" adalah pemrosesan Data Pribadi dilakukan dengan memastikan bahwa Subjek Data Pribadi telah mengetahui Data Pribadi yang diproses dan bagaimana Data Pribadi tersebut diproses, serta setiap informasi dan komunikasi yang berkaitan dengan pemrosesan Data Pribadi tersebut mudah diakses dan dipahami, dengan menggunakan bahasa yang jelas.

[9] UU PDP mengatur yang dimaksud dengan "kegagalan Pelindungan Data Pribadi" adalah kegagalan melindungi Data Pribadi seseorang dalam hal kerahasiaan, integritas, dan ketersediaan Data Pribadi, termasuk pelanggaran keamanan, baik yang disengaja maupun tidak disengaja, yang mengarah pada perusakan, kehilangan, perubahan, pengungkapan, atau akses yang tidak sah terhadap Data Pribadi yang dikirim, disimpan, atau diproses.

Dalam kondisi ini, Pengendali tidak terikat pada waktu spesifik dalam pemenuhan hak subjek data pribadi. Namun terdapat kondisi tertentu di mana pengendali harus memastikan hak subjek data pribadi terpenuhi. Hak dan kondisi tersebut adalah sebagai berikut:

1. Pelaksanaan hak penarikan persetujuan dan/atau permintaan penghapusan data pribadi yang mewajibkan pengendali menghapus data pribadi. Kewajiban penghapusan juga berlaku dalam hal pengendali tidak memerlukan data pribadi untuk mencapai tujuan pemrosesan dan/atau data pribadi diperoleh dengan cara melawan hukum. Pemberitahuan kepada subjek data wajib dilakukan kepada subjek data pribadi dalam hal pengendali melaksanakan tindakan ini.
2. Pelaksanaan hak permintaan pemusnahan data pribadi oleh subjek data pribadi. Mohon dicatat, kewajiban pemusnahan juga berlaku bagi pengendali dalam hal: masa retensi data pribadi telah habis, tidak terdapat kebutuhan penggunaan data pribadi untuk penyelesaian suatu proses perkara, dan/atau data pribadi diperoleh secara melawan hukum. Pemberitahuan kepada subjek data wajib dilakukan kepada subjek data pribadi dalam hal pengendali melaksanakan tindakan ini.
3. Pelaksanaan hak permintaan pengakhiran pemrosesan data pribadi oleh subjek data pribadi. Selain karena permintaan subjek data pribadi, pengakhiran pemrosesan juga wajib dilakukan Pengendali, dalam hal data pribadi telah mencapai masa retensi, atau tujuan pemrosesan telah tercapai.

c. *Pengecualian Pemenuhan Hak Subjek Data Pribadi*

Selain kewajiban untuk memenuhi hak subjek data pribadi, UU PDP juga mengatur beberapa kondisi di mana Pengendali dapat menolak pelaksanaan hak subjek data pribadi, sekaligus pengecualian pelaksanaan kewajiban pemenuhan hak subjek data pribadi. Kondisi tersebut sebagai berikut:

1. Penolakan pemberian akses perubahan data pribadi dalam hal membahayakan keamanan, kesehatan fisik, atau kesehatan mental Subjek Data Pribadi dan/ atau orang lain, berdampak pada pengungkapan Data Pribadi milik orang lain; dan/ atau bertentangan dengan kepentingan pertahanan dan keamanan nasional.
2. Penolakan pelaksanaan beberapa hak subjek data pribadi[10] dalam hal terdapat kepentingan pertahanan dan keamanan nasional, kepentingan proses penegakan hukum; kepentingan umum dalam rangka penyelenggaraan negara; kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem, keuangan dalam rangka penyelenggaraan negara; atau kepentingan statistik dan penelitian ilmiah.
3. Pengecualian pelaksanaan kewajiban pengendali terhadap subjek data pribadi[11] dalam hal terdapat kepentingan pertahanan dan keamanan nasional, kepentingan proses penegakan hukum; kepentingan umum dalam rangka penyelenggaraan negara; atau kepentingan pengawasan

[10] Pelaksanaan hak subjek data pribadi yang diatur dalam Pasal 8, Pasal 9, Pasal 10 ayat (1), Pasal 11, dan Pasal 13 ayat (1) dan ayat (2) UU PDP

[11] Pelaksanaan kewajiban yang diatur dalam Pasal 43 ayat (1) huruf a sampai dengan huruf c, Pasal 44 ayat (1) huruf b, Pasal 45, dan Pasal 46 ayat (1) huruf a UU PDP

sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem, keuangan dalam rangka penyelenggaraan negara.

4. Penyusunan dan Pelaksanaan Tata Kelola Pemrosesan Data Pribadi

UU PDP menekankan kegiatan pemrosesan data pribadi yang transparan, spesifik dan sah, serta sesuai dengan hukum yang berlaku. Salah satu bentuk implementasi ketentuan tersebut, dalam praktik, dilakukan oleh Pengendali dengan menyusun tata kelola pemrosesan data pribadi yang mengakomodasi ketentuan mengenai kewajiban pengendali pada saat melakukan pemrosesan. Pada umumnya, implementasinya tertuang dalam bentuk kebijakan yang mencakup ketentuan UU PDP mengenai kewajiban:

a. Melakukan perekaman seluruh kegiatan pemrosesan Data Pribadi.

b. Melindungi dan memastikan keamanan Data Pribadi yang diprosesnya melalui penyusunan dan penerapan langkah teknis operasional pemrosesan Data Pribadi dan penentuan tingkat keamanan Data Pribadi berbasis risiko Data Pribadi.

c. Menjaga kerahasiaan Data Pribadi.

d. Mengawasi setiap pihak yang terlibat pemrosesan Data Pribadi di bawah kendali Pengendali Data Pribadi.

e. melindungi Data Pribadi dari pemrosesan yang tidak sah.

f. mencegah Data Pribadi diakses secara tidak sah.

g. melakukan penilaian dampak Pelindungan Data Pribadi dalam hal pemrosesan Data Pribadi memiliki potensi risiko tinggi[12]

h. bertanggung jawab atas pemrosesan Data Pribadi, dan

i. menunjukkan pertanggungjawaban kewajiban pelaksanaan prinsip Pelindungan Data Pribadi.

5. Melaksanakan perintah lembaga dalam rangka penyelenggaraan Pelindungan data pribadi

Di samping kewajiban yang secara spesifik diatur dalam UU PDP, Pengendali sebagai subjek UU PDP juga wajib tunduk pada perintah Lembaga Pengawas Pelindungan Data Pribadi yang merupakan otoritas pengawas kegiatan pelindungan data pribadi sesuai amanat UU PDP. Kegagalan dalam menjalankan perintah Lembaga Pengawas Pelindungan Data Pribadi dapat berujung pada pengenaan sanksi.

5.3. Prinsip-Prinsip Pelindungan Data Pribadi Berdasarkan UU PDP

UU PDP disusun untuk menghadirkan pelindungan data pribadi yang komprehensif melalui penguatan hak dan prosedur pelaksanaan hak individu ketika pemrosesan data pribadi dilakukan. Selain mengatur kewajiban yang bersifat prosedural/formal, UU PDP juga mengatur prinsip pelindungan data pribadi. Prinsip tersebut disusun sebagai parameter nilai yang belum dapat direfleksikan dalam

[12] Pasal 34 UU PDP mengatur yang dimaksud dengan pemrosesan data pribadi risiko tinggi meliputi, (a) pengambilan keputusan secara otomatis yang memiliki akibat hukum atau dampak yang signifikan terhadap Subjek Data Pribadi; (b) pemrosesan atas Data Pribadi yang bersifat spesifik; (c) pemrosesan Data Pribadi dalam skala besar; (d) . pemrosesan Data Pribadi untuk kegiatan evaluasi, penskoran, atau pemantauan yang sistematis terhadap Subjek Data Pribadi; (e) pemrosesan Data Pribadi untuk kegiatan pencocokan atau penggabungan sekelompok data; (f) penggunaan teknologi baru dalam pemrosesan Data Pribadi; dan/ atau (g) pemrosesan Data Pribadi yang membatasi pelaksanaan hak Subjek Data Pribadi.

kewajiban Pengendali secara formal. Pada implementasinya, prinsip dalam UU PDP membutuhkan pengendali untuk melakukan penilaian secara komprehensif tentang bentuk pelindungan yang diwajibkan oleh UU PDP dalam implementasi kewajiban pengendali,

Adapun prinsip Pelindungan Data Pribadi dalam UU PDP :

a. pemrosesan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan;

b. pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya;

c. pemrosesan Data Pribadi dilakukan dengan menjamin hak Subjek Data Pribadi;

d. pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggung jawabkan;

e. pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, dan penghilangan Data Pribadi;

f. pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan Pelindungan Data Pribadi;

g. Data Pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan Subjek Data Pribadi, kecuali ditentukan lain oleh peraturan perundang undangan; dan

h. pemrosesan Data Pribadi dilakukan secara bertanggung jawab dan dapat dibuktikan secara jelas.

5.4. Keterkaitan UU PDP dengan Regulasi Lain

Sebagai sebuah ketentuan peraturan perundang - undangan, UU PDP tidak berdiri sendiri. Pelaksanaan berbagai ketentuan UU PDP harus dilakukan selaras dengan ketentuan lain terkait. Dalam hal ini, mengingat UU PDP mengatur tentang kegiatan pemrosesan data pribadi yang umumnya dilakukan melalui sistem elektronik, maka peraturan perundang - undangan mengenai sistem elektronik juga turut berlaku. Pelaksanaan UU PDP pun harus tetap mengindahkan ketentuan UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta ketentuan terkait.

Di samping ketentuan UU ITE dan peraturan turunannya, dalam hal terdapat ketentuan sektor dan/atau ketentuan asosiasi yang bersifat khusus mengenai kegiatan pemrosesan data pribadi, maka harus tetap dituruti berdampingan dengan kepatuhan pada UU PDP. Sebagai contoh, dalam hal terdapat ketentuan Dewan Pers, sebagai lembaga yang mengatur etika jurnalisme para jurnalis termasuk kegiatan Perusahaan Pers yang mengatur tentang isu privasi dan/atau pelindungan data pribadi, maka ketentuan tersebut harus dipatuhi.

Berangkat dari kondisi tersebut, maka Perusahaan Pers wajib mematuhi ketentuan UU PDP serta regulasi lain yang terkait kegiatan pemrosesan data pribadi baik secara langsung maupun tidak. Informasi dalam dokumen ini akan menyesuaikan kondisi tersebut untuk berupaya memberikan gambaran lengkap mengenai kewajiban Perusahaan Pers dalam peraturan perundang - undangan, serta praktik industri yang berlaku.

6. Baseline Information

Berdasarkan informasi yang dikumpulkan, dari kelima Perusahaan Pers yang menjadi sampel pada kajian ini, secara umum kelima perusahaan tersebut telah memiliki pemahaman terkait pemrosesan data pribadi. Hal ini dapat dilihat dari respon terkait jenis data pribadi yang dikumpulkan, baik data pribadi maupun spesifik, serta bentuk persetujuan dalam pemrosesan data pribadi.

Perbedaan jenis data pribadi yang diproses dapat mengakibatkan timbulnya kewajiban hukum kepada Perusahaan Pers sebagai pengendali data pribadi pada saat melakukan pemrosesan data pribadi, serta penerapan kebijakan manajemen informasi dan langkah pelindungan yang sesuai dengan data pribadi/aset Perusahaan Pers yang ingin dilindungi.

Berdasarkan kuesioner dan reviu yang telah dilakukan terhadap 5 Perusahaan Pers sampel (yaitu Tempo, Tribunnews Group, Dari Laut, Batamnews, dan Berita Jatim), ditemukan bahwa terdapat potensi:

a. Pemrosesan data pribadi yang masih belum optimal atau terkelola dengan baik, karena ada *misalignment* pemahaman tentang proses pemanfaatan dan pengelolaan data pribadi yang dikumpulkan;

b. Penerapan fitur atau teknologi dalam situs/platform yang dikelola oleh Perusahaan Pers belum dimanfaatkan atau dipahami secara optimal oleh unit kerja yang mengelola sehingga belum sesuai dengan persyaratan peraturan pelindungan data pribadi di Indonesia, berdasarkan kondisi tidak sinkronnya respon antara kuesioner dengan temuan fitur di situs Perusahaan Pers;

c. Penerapan fitur yang berlaku secara regional di luar wilayah Indonesia, namun tidak berlaku di wilayah Indonesia, padahal memiliki fungsi yang dapat membantu Perusahaan Pers meningkatkan kepatuhan terhadap persyaratan peraturan pelindungan data pribadi.

Pada tahap tata kelola pelindungan data pribadi, masih banyak ditemukan ruang untuk dilakukan peningkatan, khususnya, antara lain:

a. Informasi terkait komitmen pelindungan data pribadi kepada Subjek Data yang dituangkan dalam kebijakan privasi (*privacy notice*) masih belum memenuhi ketentuan dalam peraturan pelindungan data pribadi di Indonesia;

b. Penyesuaian dasar pemrosesan data pribadi agar tidak lagi bertumpu pada persetujuan;

c. Belum adanya kebijakan internal terkait pelindungan data pribadi yang dimiliki oleh Perusahaan Pers meliputi mekanisme kontrol terhadap pihak terkait kegiatan pengendalian data pribadi, pelaksanaan *data protection impact assessment* untuk pemrosesan data spesifik, dan *data transfer impact assessment* untuk pengiriman data pribadi ke luar wilayah Indonesia;

d. Fokus tata kelola pelindungan data pribadi hanya terbatas pada data pribadi konsumen, namun data pribadi karyawan dan penyedia jasa belum terkelola secara jelas; dan

e. Masih beragamnya pemahaman lintas divisi pada Perusahaan Pers terkait kegiatan pemrosesan data pribadi.

Adapun untuk ke-50 Perusahaan Pers yang mengisi kuesioner, jika dibandingkan dengan lima media sampel, maka dapat ditemukan informasi dan analisis sebagai berikut:

a. Hampir keseluruhan Perusahaan Pers yang mengisi kuesioner menganggap memiliki pemahaman terkait konteks kegiatan pelindungan data pribadi. Hal ini terlihat dari jawaban tidak tahu yang rata - rata dijawab oleh Perusahaan Pers untuk setiap

pertanyaan dibawah 30%. Beberapa pertanyaan tersebut misalnya “Apakah Perusahaan Pers memproses data pribadi?”, “Apakah Perusahaan Pers telah mendapatkan persetujuan Subjek Data Pribadi?” dan pertanyaan sejenis. Respon tidak tahu dari pertanyaan tersebut menunjukan bahwa Perusahaan Pers memiliki pemahaman (meski masih umum dan belum terlalu detail pada pelaksanaan) terhadap pemrosesan data pribadi.

b. Sebesar 76% Perusahaan Pers melakukan kegiatan pemrosesan data pribadi yang dengan menggunakan dasar pemrosesan persetujuan. Namun, 46% Perusahaan Pers tidak memiliki kebijakan privasi, sebagai salah satu metode pemberian informasi mengenai pemrosesan data pribadi yang dilakukan. Hal ini menimbulkan ketidaksesuaian antara praktik Perusahaan Pers dengan kewajiban penggunaan persetujuan sebagai dasar pemrosesan data pribadi sesuai UU PDP.

c. Dari berbagai kegiatan pemrosesan data pribadi oleh Perusahaan Pers, terdapat banyak tujuan pemrosesan yang dapat menggunakan berbagai dasar pemrosesan data pribadi selain persetujuan. Terlebih, dari ke-50 Perusahaan Pers dalam kuesioner kali ini tidak semuanya menjawab telah mendapatkan persetujuan dari subjek data pribadi ketika memproses data pribadi, atau tidak memiliki kebijakan privasi.

d. Terdapat kebutuhan peningkatan pemahaman tentang ragam bentuk data pribadi serta konsekuensi pemrosesan data pribadi di antara 50 Perusahaan Pers. Hal ini didasari respon beberapa Perusahaan Pers yang menganggap pihaknya tidak melakukan pemrosesan data pribadi spesifik berupa golongan darah, padahal memproses data pribadi berupa KTP yang mengandung informasi golongan darah subjek data pribadi. Beberapa Perusahaan Pers mengetahui bahwa golongan darah merupakan data pribadi spesifik, namun masih lebih banyak yang belum menyertakan pemahaman tersebut dalam kegiatan pemrosesan data pribadinya.

e. Kegiatan pemrosesan data pribadi berupa golongan darah ini juga menunjukan kondisi pemahaman Perusahaan Pers terhadap pelaksanaan prinsip pemrosesan data pribadi secara terbatas dan spesifik (*data minimization principle*). Prinsip tersebut pada intinya menekankan bahwa pemrosesan data pribadi harus dilakukan secara terbatas sesuai dengan tujuan pemrosesan data pribadi. Dalam hal Perusahaan Pers memproses data pribadi lebih dari yang diperlukan, maka dapat dianggap melanggar prinsip ini dan meningkatkan risiko bagi Perusahaan Pers. Kondisi ini juga terlihat dari 24% Perusahaan Pers yang memproses data pribadi berupa catatan kejahatan subjek data pribadi. Perlu diperiksa lebih jauh tujuan pemrosesan data pribadi ini.

f. Peningkatan pemahaman terkait ragam bentuk kegiatan pemrosesan data pribadi juga diperlukan. Hal ini mengingat 90% dari Perusahaan Pers menggunakan fitur Google Analytics tapi 76% Perusahaan menganggap tidak melakukan pengiriman data ke pihak lain. Namun, apabila merujuk pada praktik penerapan peraturan perundang - undangan di Uni Eropa, penggunaan Google Analytics dianggap sebagai suatu bentuk pengiriman data pribadi.[13]

g. Kondisi pemahaman terkait kegiatan pemrosesan data pribadi juga terlihat dalam kegiatan penyimpanan data pribadi. Sebanyak 48% Perusahaan Pers mengatakan bahwa penyimpanan dilakukan dalam Google Drive, namun 80% menganggap bahwa kegiatan penyimpanan yang dilakukannya tidak dilakukan oleh pihak ketiga. Hal ini menunjukan bahwa Perusahaan Pers belum memahami posisi Google sebagai penyedia Google Drive merupakan perusahaan IT penyedia layanan yang sebetulnya merupakan pihak ketiga dalam kegiatan pemrosesan data pribadi.

---

[13] Google, 2024, *Regarding international data transfers in Google Analytics* <https://support.google.com/analytics/answer/11609059?hl=en> diakses pada 5 April 2024

h. Peningkatan pemahaman terhadap konsekuensi dari pemrosesan data pribadi spesifik juga masih diperlukan. Sebanyak 56% Perusahaan Pers menjawab tidak pernah melakukan analisis dampak pemrosesan data pribadi, sedangkan 22% menjawab tidak tahu. Hanya 22% Perusahaan Pers melakukan analisis dampak pemrosesan data pribadi karyawan. Kondisi tersebut kontras dengan respon 60% Perusahaan Pers yang melakukan pemrosesan data pribadi berupa rekening karyawan yang merupakan pemrosesan data pribadi spesifik. Selain itu juga terdapat beragam pemrosesan data pribadi spesifik dalam berbagai bentuk. Perlu dicatat, verifikasi lebih lanjut untuk memahami kegiatan analisis yang dilakukan dan kesesuaian kegiatan analisis diperlukan.

i. Sekitar 42% media menyatakan memiliki kebijakan internal sedangkan 46% mengatakan tidak. Namun jika melihat respon lebih lanjut ada potensi kerancuan antara *privacy policy, privacy notice,* dan kebijakan penggunaan data perusahaan. Pada praktiknya memang dokumen tersebut memiliki potensi tercampur antara kebijakan keamanan informasi dan pemrosesan data pribadi sehingga perlu ditelaah lebih lanjut.

j. Sebanyak 80% Perusahaan Pers menjawab bahwa pemrosesan data pribadi (termasuk penyimpanan dan pengelolaan) dilakukan oleh internal. Namun beberapa jawaban selanjutnya ditemukan bahwa 48% dari Perusahaan Pers yang menyimpan datanya di layanan komputasi awan. Sehingga bukan tidak mungkin pemrosesan yang dianggap internal tetap melibatkan teknologi/instrumen yang sebetulnya dapat dianggap melibatkan pihak ketiga. Untuk Perusahaan Pers, yang menjawab menggunakan pihak ketiga, 81.3% dari pihak yang menggunakan pihak ketiga dalam pemrosesan data pribadi untuk keperluan penyimpanan menjawab tidak punya perjanjian kerja sama. Hal ini dapat diinterpretasikan bahwa Perusahaan Pers tersebut tidak memiliki perjanjian namun bisa jadi memang tidak ada, atau ada namun tidak sadar bahwa perjanjian tersebut berlaku.

k. Pengiriman data pribadi oleh Perusahaan Pers dilakukan untuk tujuan pemenuhan kewajiban kepada karyawan, keperluan periklanan, dan analisis peningkatan layanan. Pengiriman data tersebut biasanya dilakukan via email, dan/atau aplikasi pesan singkat. Bentuk pengirimannya dilakukan melalui dokumen dengan fail ekstensi .doc, .xls, dan/atau .txt. Meskipun tidak secara spesifik kegiatan ini adalah praktik yang dianggap melanggar UU PDP, namun pemilihan model pengiriman data pribadi melalui email dan/atau aplikasi pesan singkat membutuhkan tambahan upaya keamanan (Misal: melalui email terenkripsi, akses email penerima dan pengirim yang terbatas, dan lain sebagainya) untuk menghadirkan pelindungan data pribadi yang lebih baik.

7. Gap Assessment

Pada bagian ini akan dijelaskan kesenjangan antara kondisi *existing* Perusahaan Pers sesuai dengan *baseline information* dibandingkan kondisi ideal yang disyaratkan oleh peraturan perundang - undangan yang berlaku serta praktik industri pada umumnya.

Pemahaman Postur Pemrosesan Data Pribadi	
Kondisi Saat Ini	● Perusahaan Pers telah mengetahui sumber (dikumpulkan langsung dari subjek data pribadi seperti konsumen, karyawan, dan vendor) serta tipe data pribadi, namun belum melakukan kewajiban pemrosesan data pribadi spesifik sesuai UU PDP. ● Perusahaan Pers melakukan kegiatan pemrosesan data pribadi untuk memenuhi tujuan pemrosesan data pribadi, termasuk diantaranya melakukan pengiriman data pribadi kepada pihak lain.

Level Minimum Kepatuhan	● Perusahaan Pers selaku Pengendali Data Pribadi diwajibkan untuk memahami postur (kondisi keseluruhan) pemrosesan data pribadi yang terjadi, termasuk jenis data pribadi yang diproses, pihak terkait, posisi serta relasi Perusahaan Pers dengan pihak lain dalam kegiatan pemrosesan data pribadi.
Rekomendasi	● Mengetahui jenis data pribadi yang dikumpulkan oleh Perusahaan Pers untuk mengantisipasi kewajiban hukum Perusahaan Pers pemrosesan data pribadi, serta penerapan kebijakan dan langkah pelindungan yang sesuai. ● Memeriksa asal data pribadi yang dikumpulkan apakah dikumpulkan langsung dari subjek data pribadi atau menerima data pribadi dari pihak lain. ● Memeriksa kategori subjek data pribadi yang dikumpulkan data pribadinya. ● Memetakan kegiatan Pemrosesan Data Pribadi yang dilakukan Perusahaan Pers dengan memetakan peran dan tanggung jawab pihak dalam maupun luar perusahaan yang memiliki terlibat pada pemrosesan data pribadi Perusahaan Pers, termasuk pemetaan perangkat dan/atau instrumen yang digunakan dalam pemrosesan data pribadi. ● Memeriksa posisi perusahaan dalam kegiatan pemrosesan data pribadi apakah sebagai pengendali, prosesor, atau hubungan yang timbul (bisa pengendali ke pengendali, pengendali bersama, atau pengendali ke prosesor). ● Melakukan reviu dokumen, produk, atau keluaran yang berpotensi mengandung data pribadi untuk memahami potensi publikasi data pribadi, sebagai bagian pemrosesan data pribadi.

Dasar Pemrosesan Data Pribadi	
Kondisi Saat Ini	● Beberapa Perusahaan Pers menggunakan persetujuan sebagai dasar pemrosesan data pribadi. ● Persetujuan dikumpulkan melalui perjanjian dengan karyawan dan/atau vendor atau pada saat konsumen mendaftar pada layanan Perusahaan Pers. ● Informasi persetujuan pada umumnya disampaikan melalui dokumen kebijakan privasi (*privacy notice*) meski tidak semua Perusahaan Pers memiliki dokumen *privacy notice*. ● Informasi permintaan persetujuan belum menyertakan informasi yang diwajibkan oleh UU PDP. ● Metode permintaan persetujuan belum memfasilitasi subjek data pribadi untuk memberikan persetujuan secara eksplisit. ● Beberapa Perusahaan Pers tidak memiliki dokumen *privacy notice.*
Level Minimum Kepatuhan	● Persetujuan pemrosesan harus dilakukan melalui adanya persetujuan tertulis atau terekam. ● Persetujuan dilakukan secara *opt-in* dan eksplisit dimana subjek data pribadi harus memberikan persetujuan secara afirmatif, berdasarkan tindakan atau pernyataan yang secara terang menjelaskan persetujuan subjek data pribadi terhadap pemrosesan data pribadi.

Rekomendasi	● Menentukan dasar pemrosesan data pribadi yang sesuai tujuan Perusahaan Pers dalam melakukan pemrosesan data pribadi serta kewajiban hukum yang dapat dilakukan oleh Perusahaan Pers ● Membuat salah satu *database* yang dikhususkan untuk menyimpan *metadata consent* yang direkam secara digital. Minimum, metadata tersebut terdiri dari: *timestamp*, jenis data pribadi yang dikumpulkan/proses, tujuan, *user identifier* (seperti *user ID*), *status consent*, dan kalimat persetujuan/*consent statement*. ● Dalam hal dasar pemrosesan data pribadi menggunakan kepentingan yang sah sebagai dasar pemrosesan data pribadi, maka pengendali perlu menyiapkan *Legitimate Interest Assessment*. ● Dalam hal dasar pemrosesan data pribadi menggunakan persetujuan maka perlu untuk: ○ Menyiapkan mekanisme pengumpulan persetujuan subjek Data sebelum pemrosesan dilakukan, tergantung subjek data pribadi yang memberikan persetujuan, misalnya: ■ untuk data pribadi karyawan, pengumpulan persetujuan karyawan dapat dilaksanakan pada saat penandatanganan perjanjian kerja. ■ untuk data pribadi konsumen, pengumpulan persetujuan dilaksanakan dengan menyediakan check-box yang menyatakan konsumen menyetujui pemrosesan data pribadi pada kesempatan pertama sebelum terjadi pemrosesan data pribadi. ■ untuk data pribadi vendor, pengumpulan persetujuan dilaksanakan pada saat penandatanganan perjanjian kerja sama, penyediaan jasa atau dokumen serupa. ○ Menyampaikan informasi (biasanya dalam bentuk Dokumen Kebijakan Privasi) menggunakan bahasa Indonesia, paling sedikit berisi: ■ Jenis data pribadi, informasi dan relevansi pengumpulan informasi dan data pribadi tersebut, ■ Tujuan pemrosesan data pribadi, ■ Dasar hukum pemrosesan data pribadi, ■ Jangka waktu penyimpanan data pribadi, ■ Hak subjek data pribadi, ■ Narahubung yang dapat dihubungi, ■ Pihak yang terlibat kegiatan pemrosesan data pribadi. ■ Ketentuan pembaruan Kebijakan Privasi, ■ Kegiatan pemrosesan data pribadi yang dilakukan, dan ■ Ketentuan jika terjadi kegagalan pelindungan data pribadi.

Pengawasan Kegiatan Pemrosesan Data Pribadi	
Kondisi Saat Ini	● Perusahaan Pers belum memiliki kebijakan internal tata kelola data pribadi, serta mekanisme pengawasan terhadap pihak - pihak yang terlibat dalam pemrosesan data pribadi. ● Belum ditemukan Perusahaan Pers yang secara spesifik telah menunjuk pejabat pelindungan data pribadi.

Level Minimum Kepatuhan	● Pengendali untuk memiliki pejabat pelindungan data pribadi ● Memiliki kebijakan tata kelola data pribadi yang berisi langkah operasional teknis pelindungan data pribadi dari gangguan pemrosesan data pribadi. ● Memiliki metode pengawasan kegiatan pemrosesan data pribadi berupa: (i) rekam pemrosesan data pribadi, (ii) perjanjian pemrosesan data pribadi, dan (iii) mekanisme audit.
Rekomendasi	● Menunjuk Pejabat Pelindungan Data Pribadi yang bertugas memantau dan memastikan kepatuhan Pengendali dan Prosesor dalam kegiatan pemrosesan data pribadi. ● Menyiapkan Kebijakan Privasi (*Privacy Notice*) bagi Subjek Data untuk memberikan pemberitahuan pemrosesan data pribadi dengan detail informasi sesuai poin Rekomendasi pada Bagian Dasar Pemrosesan Data Pribadi ● Menyusun Kebijakan Internal Pemrosesan Data Pribadi yang paling sedikit memuat informasi: ○ Jenis dan ragam data pribadi yang diproses oleh Perusahaan Pers; ○ Pembagian tanggung jawab pihak internal dalam pemrosesan data pribadi; ○ Kewajiban Perusahaan Pers kepada subjek data pribadi; ○ Mekanisme penanganan pelaksanaan hak subjek data pribadi; ○ Ketentuan respon dalam hal terjadi kegagalan pelindungan data pribadi; ○ Ketentuan pelibatan pihak ketiga dalam pemrosesan data pribadi; ○ Bentuk kegiatan pemrosesan data pribadi yang dilakukan oleh organisasi; ○ Jangka waktu penyimpanan data pribadi; ○ Larangan serta kewajiban individu yang terlibat dalam pemrosesan data pribadi; ○ Pemrosesan data pribadi yang diterima dari selain subjek data; ○ Mekanisme pengiriman data pribadi ke pihak lain di dalam dan luar negeri; ○ Mekanisme ketika organisasi melakukan pemisahan, pengambilalihan, peleburan, penggabungan, dan pembubaran badan hukum; ○ Mekanisme audit, prosedur pengoperasian, tugas, wewenang, dan kontak pejabat pelindungan data pribadi; ○ Manajemen keamanan informasi dan insiden keamanan informasi yang mencakup proses dan peran dan tanggung jawab karyawan dalam hal terjadi insiden keamanan; ● Menyiapkan Perekaman Kegiatan Pemrosesan Data Pribadi / *Record of Processing Activities* (RoPA) sebagai bentuk inventarisasi kegiatan pemrosesan data pribadi yang dilakukan oleh Pengendali Data Pribadi. ● Menyiapkan perjanjian standar untuk pihak ketiga yang memproses data pribadi dengan menyertakan jaminan pelindungan data pribadi terhadap data pribadi yang disediakan oleh organisasi dapat berupa kerja sama dengan pihak lain sebagai prosesor, kerja sama untuk pengiriman data, kerja sama pengendalian bersama (*Joint Controller*) atau bentuk kerja sama lainnya.

	● Menyediakan kanal komunikasi bagi pengguna jika terdapat keluhan atau kebutuhan pengguna melaksanakan hak sebagai subjek data dalam UU PDP.

Kerahasiaan Data Pribadi	
Kondisi Saat Ini	● Tidak dilakukannya enkripsi atas data pribadi yang diproses oleh Perusahaan Pers.
Level Minimum Kepatuhan	● Perusahaan Pers selaku Pengendali Data Pribadi diwajibkan untuk menjaga kerahasiaan data pribadi dan melindungi data pribadi dari pemrosesan yang tidak sah.
Rekomendasi	● Melakukan segregasi dan klasifikasi data pribadi yang diproses oleh Perusahaan Pers yang dapat dicantumkan dalam kebijakan pelindungan data pribadi. ● Melakukan enkripsi dan/atau *data masking* atas data pribadi yang diproses dan dikelola oleh Perusahaan Pers. ● Mengimplementasikan *user access matrix* untuk memastikan bahwa hanya karyawan-karyawan tertentu dan berkepentingan saja yang dapat mengakses data pribadi, baik akses secara fisik maupun secara digital. ● Mengimplementasikan *multifactor authentication* untuk memastikan bahwa karyawan atau personel bersangkutan yang akan mengakses data pribadi. ● Terdapat *audit log* atau *trail log* atas aktifitas yang dilakukan oleh karyawan atau personel atas data pribadi (seperti: melihat, menghapus, mereplikasi, dan lainnya). *Audit log* tersebut harus direviu setidaknya sekali dalam setahun untuk memastikan bahwa akses terhadap data pribadi diberikan kepada karyawan yang relevan ● Membuat dan mengimplementasikan ketentuan klasifikasi. informasi (*information classification policy*) yang mendefinisikan bagaimana penanganan dan langkah keamanan yang harus diimplementasikan atas bentuk informasi tertentu. ● Memastikan setiap karyawan atau personel telah menandatangani perjanjian kerahasiaan untuk mencegah adanya pengungkapan data pribadi. ● Perusahaan Pers wajib memastikan bahwa pihak ketiga yang melakukan pemrosesan data pribadi atas nama Perusahaan Pers (jika ada) memiliki level keamanan yang mumpuni untuk menjaga kerahasiaan data pribadi. Hal ini dapat dilakukan dengan melakukan pengawasan atas pihak ketiga tersebut. ● Melakukan *penetration testing* atas sistem secara berkala.

Transfer Data Pribadi	
Kondisi Saat Ini	● Perusahaan Pers melakukan pengiriman atau transfer data pribadi ke pihak ketiga untuk memenuhi tujuan pemrosesan.
Level Minimum Kepatuhan	● Perusahaan Pers harus memastikan bahwa negara dan pihak ketiga yang menerima data pribadi tersebut memiliki tingkat

	pelindungan data pribadi yang setara atau lebih tinggi, serta memadai.
Rekomendasi	● Melakukan *data transfer impact assessment* atau penilaian atas setiap kegiatan pengiriman data pribadi ke pihak ketiga (baik di dalam negeri maupun di luar negeri). ● Memastikan bahwa metode pengiriman data pribadi yang dipilih merupakan metode pengiriman yang aman, seperti *Application Programming Interface (API)* dengan mengimplementasikan langkah-langkah keamanan yang sesuai (contoh: enkripsi saat *data at-rest* dan *in-transit*). ● Memastikan terdapat perjanjian pemrosesan data pribadi antara Perusahaan Pers dengan pihak ketiga yang akan memproses data pribadi tersebut.

Keamanan Sistem	
Kondisi Saat Ini	● Tidak ada informasi terkait sertifikasi keamanan sistem informasi yang dimiliki oleh Perusahaan Pers. ● Pengamanan sistem oleh Perusahaan Pers baru berupa pembatasan akses dan enkripsi.
Level Minimum Kepatuhan	● Perusahaan Pers diwajibkan untuk melindungi keamanan data pribadi dari akses yang tidak sah, pengungkapan yang tidak sah, penyalahgunaan, perusakan, dan/atau menghilangnya data pribadi.
Rekomendasi	● Memiliki kebijakan terkait dengan keamanan informasi. ● Menerapkan keamanan informasi pada setiap fase kepegawaian. Hal ini mencakup verifikasi latar belakang calon karyawan, melakukan pelatihan keamanan informasi, adanya proses disiplin dalam hal terjadi kebocoran data, dan ketentuan keamanan informasi setelah karyawan tersebut tidak lagi menjadi bagian dari perusahaan. ● Melakukan identifikasi atas setiap aset perusahaan yang berkaitan dengan manajemen informasi dan menetapkan langkah pelindungan yang sesuai. ● Melakukan kontrol atas akses terhadap informasi melalui *user management*. ● Memastikan keamanan, integritas, dan ketersediaan data melalui adanya kebijakan terkait kriptografi. ● Memiliki kebijakan terkait dengan keamanan operasional yang mencakup namun tidak terbatas kepada *backup*, *logging and monitoring*, *penetration testing*, keamanan terhadap *malware*, dan *vulnerability management*. ● Memiliki manajemen atas insiden keamanan informasi. Hal ini mencakup proses dan peran dan tanggung jawab karyawan dalam hal terjadi insiden keamanan ● Memiliki dokumen terkait dengan *Business Continuity* dan *Disaster Recovery* yang mencakup keberlangsungan bisnis dalam hal terdapat hal-hal yang tidak diinginkan terjadi ● Memasukkan aspek-aspek privasi dalam pengembangan perangkat lunak atau *software development lifecycle.*

Penilaian Dampak Pemrosesan Data Pribadi	
Kondisi Saat Ini	● Perusahaan Pers melakukan pemrosesan data pribadi spesifik yang membutuhkan penilaian dampak pemrosesan data pribadi. ● Tidak ada informasi mengenai kegiatan penilaian dampak pemrosesan data pribadi yang dilakukan Perusahaan Pers sebelum melakukan pemrosesan data pribadi spesifik.
Level Minimum Kepatuhan	● Pengendali wajib melakukan penilaian dampak Pelindungan Data Pribadi dalam hal pemrosesan Data Pribadi memiliki potensi risiko tinggi terhadap Subjek Data Pribadi, salah satunya dalam hal pemrosesan data pribadi spesifik.
Rekomendasi	● Melakukan penilaian dampak pemrosesan data pribadi yang mengandung informasi terkait: ○ Deskripsi secara sistematis mengenai kegiatan pemrosesan Data Pribadi dan tujuan pemrosesan Data Pribadi, termasuk kepentingan dari Pengendali Data Pribadi dari pemrosesan data pribadi; ○ Penilaian kebutuhan dan proporsionalitas antara tujuan dan kegiatan pemrosesan Data Pribadi; ○ Penilaian risiko terhadap pelindungan hak Subjek Data Pribadi; dan ○ Langkah yang digunakan Pengendali Data Pribadi untuk melindungi Subjek Data Pribadi dari risiko pemrosesan Data Pribadi.

Pemberitahuan Kegagalan Pelindungan Data Pribadi	
Kondisi Saat Ini	● Tidak ada informasi terkait pemberitahuan kegagalan data pribadi yang dilakukan oleh Perusahaan Pers. ● Tidak ada informasi yang ditemukan di ranah publik mengenai kegagalan pelindungan data pribadi yang dialami Perusahaan Pers.
Level Minimum Kepatuhan	● Pengendali wajib mengirimkan notifikasi kegagalan pelindungan data pribadi kepada subjek data pribadi dan lembaga PDP.
Rekomendasi	● Dokumen notifikasi kegagalan pelindungan data pribadi kepada subjek data pribadi dan lembaga PDP yang berisi informasi: ○ Data Pribadi yang terungkap; ○ Deskripsi jenis kegagalan Pelindungan Data Pribadi; ○ Waktu dan cara Data Pribadi terungkap; ○ Dampak kegagalan Pelindungan Data Pribadi terhadap Subjek Data Pribadi; ○ Upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi; dan ○ Informasi narahubung.

Peningkatan Kemampuan Pihak Terkait Pemrosesan Data Pribadi

Kondisi Saat Ini	● Tidak ada informasi tentang kegiatan peningkatan kemampuan pihak terkait pemrosesan data pribadi dilakukan oleh Perusahaan Pers.
Level Minimum Kepatuhan	● Pengendali data, sebagai penyelenggara sistem elektronik, wajib mendidik dan melatih personil yang bertugas dan bertanggung jawab terhadap pengamanan dan pelindungan sarana dan prasarana sistem elektronik.
Rekomendasi	● Melakukan Pelatihan terkait hal - hal yang perlu diperhatikan dalam pemrosesan data pribadi serta keamanan sistem elektronik bagi individu yang terlibat dalam pemrosesan data pribadi. ● memberikan pemahaman bagi karyawan atau personel terkait pentingnya kerahasiaan data pribadi, termasuk melalui pengenaan kewajiban penandatanganan perjanjian kerahasiaan oleh karyawan yang bertanggung jawab pada pemrosesan data pribadi.

8. Kesimpulan dan rekomendasi

Dari hasil analisis di atas ditemukan bahwa kegiatan pemrosesan data pribadi yang cukup krusial untuk menjadi perhatian Perusahaan Pers adalah pemrosesan data pribadi karyawan. Kondisi ini berlaku baik untuk lima media sampel, maupun 50 Perusahaan Pers. Meskipun data pribadi konsumen memiliki tingkat urgensitas yang signifikan, namun kegiatan pemrosesannya lebih banyak dipahami oleh para media. Hal ini memberikan kesempatan untuk peningkatan praktik secara lebih optimal. Terlebih, dari media yang mengisi kuesioner ini, ragam bentuk pemrosesan terhadap data pribadi konsumen masih cukup terbatas dibandingkan dengan pemrosesan terhadap karyawan yang pada umumnya melibatkan pihak lain.

Oleh karena itu, sebagai bentuk rekomendasi, Perusahaan Pers perlu mempertimbangkan untuk meningkatkan kebijakan, standar, dan praktik pelindungan data pribadi karyawannya. Secara paralel, standar yang telah ditingkatkan tersebut dapat memberikan *spillover effect* pada pelindungan data pribadi konsumen. Peningkatan tersebut dapat dilakukan melalui peningkatan kebijakan, adopsi teknologi, serta sumber daya manusia. Upaya untuk mengorkestrasi peningkatan praktik dan kebijakan tersebut dapat dilakukan secara individual maupun bersama - sama, dalam hal ini di bawah koordinasi AMSI.

9. Penutup

Demikian laporan ini disusun untuk dapat menjadi pertimbangan pihak - pihak terkait, khususnya dalam meningkatkan praktik pelindungan data pribadi Perusahaan Pers di lingkungan AMSI.

Referensi

Gargiulo, M. ‘Council Post: Data Security Threats: What You Need To Know.’ Forbes, May 16 2022 <https://www.forbes.com/sites/forbestechcouncil/2022/05/16/data-security-threats-what-you-need-to-know/>. Diakses 17 Februari 2024.

Google 2024. ‘Regarding international data transfers in Google Analytics’ <https://support.google.com/analytics/answer/11609059?hl=en> diakses pada 5 April 2024

Hancock, J 2020. ‘Psychology of Human Error,' Joint Study from Stanford University and Tessian.

Park, Colleen McClain, Michelle Faverio, Monica Anderson and Eugenie. ‘How Americans View Data Privacy.’ Pew Research Center, 18 Oktober 2023, <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>. Diakses 18 Februari 2024.

Riset survei nasional Kementerian Kominfo dan Katadata Insight Center, 2020. ‘'Persepsi Masyarakat atas Pelindungan Data Pribadi’

Lampiran

Lampiran - Compliance Checklist Pelindungan Data Pribadi AMSI

Kualifikasi:

1. Dokumen ini merupakan dokumen yang bersifat panduan, tidak mengikat secara hukum, dan hanya memberikan penjelasan langkah – langkah praktis tata kelola pelindungan data pribadi. Dokumen ini bukan merupakan suatu nasihat hukum sehingga pemanfaatan dan penggunaannya tidak menjadi tanggung jawab penyusun.
2. Dokumen ini disusun berdasarkan analisis terhadap kebutuhan pemenuhan kewajiban pelindungan data pribadi yang dikumpulkan dari lima Perusahaan pers anggota AMSI. Pemakaian oleh pihak selain lima Perusahaan pers anggota AMSI membutuhkan penyesuaian yang mungkin saja belum terakomodasi dalam dokumen ini.
3. Dokumen ini disusun dengan merujuk peraturan perundang – undangan terkait, praktik industri serta rancangan peraturan perundang – undangan. Mengingat sifat rujukan rancangan peraturan perundang – undangan dapat berubah, maka pengguna dokumen ini perlu untuk memastikan kesesuaian dan keterbaruan informasi yang berlaku dalam dokumen ini.

Petunjuk Penggunaan:

Checklist ini memberikan informasi teknis dan praktis yang dapat diikuti oleh pembacanya dalam menghadirkan tata kelola data pribadi pada organisasinya. *Point of view* checklist ini diambil dari sudut pandang pengendali data pribadi. Meskipun beberapa informasi dalam dokumen ini cukup detil, beberapa informasi teknis dari peraturan perundang - undangan tidak disertakan untuk efisiensi dokumen. Pengguna dokumen ini diminta untuk tetap memastikan kesesuaian informasi dari checklist ini dengan ketentuan peraturan perundang – undangan yang berlaku.

Keluaran dari checklist ini adalah daftar aksi yang perlu dilakukan, dalam bentuk implementasi teknis dan penyediaan aturan internal, kebijakan (policy), atau prosedur standar operasi (SOP), untuk melengkapi persyaratan kepatuhan terhadap UU PDP.

Kolom Status dapat diisi dengan tingkat kepatuhan terhadap UU PDP atas subjek bahasan. Pada subjek-subjek bahasan yang belum memenuhi aturan kepatuhan perlu dibuat rencana aksi pemenuhannya yang akan menjadi keluaran checklist ini.

Checklist:

No.	Kewajiban Pelindungan Data Pribadi	Status
1.	**Memeriksa Keberlakuan UU PDP terhadap Perusahaan Pers**	
2.	**Mengetahui jenis data pribadi yang dikumpulkan oleh Perusahaan Pers** 2.1. Sesuai UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, data pribadi terdiri atas: ● Data pribadi bersifat spesifik meliputi, data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi dan/atau data lain sesuai ketentuan peraturan perundang-undangan. ● Data pribadi bersifat umum meliputi, nama lengkap, jenis kelamin,	

	kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasikan seseorang. Selain data pribadi spesifik, maka data pribadi lain dianggap bersifat umum. 2.2. Perbedaan jenis data pribadi yang diproses dapat mengakibatkan timbulnya kewajiban hukum kepada Perusahaan Pers sebagai pengendali data pribadi pada saat melakukan pemrosesan data pribadi, serta penerapan kebijakan manajemen informasi dan langkah pelindungan yang sesuai dengan data pribadi/aset Perusahaan Pers yang ingin dilindungi.	
3.	**Memeriksa asal data pribadi yang dikumpulkan** Data Pribadi dapat dikumpulkan langsung oleh Perusahaan Pers dari individu sebagai subjek data pribadi di berbagai kesempatan, atau Perusahaan Pers menerima data pribadi. Perbedaan asal data pribadi dapat menimbulkan perbedaan posisi dan kewajiban hukum Perusahaan Pers.	
4.	**Memeriksa kategori subjek data pribadi yang dikumpulkan data pribadinya** 4.1. Kategori subjek data pribadi yang diproses data pribadinya oleh Perusahaan Pers meliputi konsumen yang mendaftarkan diri menjadi pelanggan layanan Perusahaan Pers, karyawan yang menandatangani perjanjian kerja, penyedia jasa/barang bagi Perusahaan Pers yang menandatangani perjanjian kerja sama. 4.2. Secara normatif tidak terdapat perbedaan kewajiban, namun secara teknis Perusahaan Pers dapat memiliki jalur komunikasi, penanggungjawab pemrosesan data pribadi, serta ketentuan teknis lain yang berbeda tergantung kategori subjek data pribadi.	
5.	**Melakukan Pemetaan Ragam Kegiatan Pemrosesan Data Pribadi yang dilakukan Perusahaan Pers** 5.1. Pemetaan kegiatan pemrosesan data pribadi dilakukan dengan membuat diagram pemrosesan data pribadi sejak pengumpulan data pribadi dilaksanakan serta bentuk kegiatan pemrosesan data pribadi yang dilakukan oleh Perusahaan Pers. 5.2. Pemetaan juga dilakukan dengan memetakan pihak dalam maupun luar perusahaan yang memiliki akses dan terlibat pada kegiatan pemrosesan data pribadi Perusahaan Pers sehingga peran dan tanggung jawab setiap pihak dalam kegiatan pemrosesan data pribadi Perusahaan Pers dapat diketahui. 5.3. Kegiatan ini juga dapat dilengkapi dengan alat, instrumen, perangkat, *software* dan/atau fitur yang digunakan untuk memproses data pribadi oleh perusahaan. Melalui pemetaan ini, Perusahaan Pers dapat memahami data pribadi yang diproses oleh instrumen pemroses data pribadi, kebijakan penggunaan yang menjadi dasar pemanfaatan instrumen pemroses data pribadi, serta dapat memperkirakan risiko yang dapat terjadi pada saat pemrosesan data pribadi dilakukan.	
6.	**Memeriksa posisi perusahaan dalam kegiatan pemrosesan data pribadi** 6.1. Pemeriksaan posisi dapat dilakukan dengan memahami tugas, peran, dan tanggung jawab Perusahaan Pers dalam pemrosesan data pribadi. UU PDP mengatur bahwa pengendali data pribadi merupakan pihak yang menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi, sedangkan prosesor data pribadi adalah pihak yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan Data	

	Pribadi atas nama Pengendali Data Pribadi. Perbedaan posisi ini dapat mempengaruhi tanggung jawab hukum Perusahaan Pers dalam pemrosesan data pribadi. 6.2. Pada praktiknya pemeriksaan dapat dilakukan dengan memeriksa perjanjian kerja sama yang menjadi dasar terjadinya kegiatan pemrosesan data pribadi yang dilakukan dengan pihak lain. Dalam hal tidak ada pihak lain yang memiliki kewenangan menetapkan tujuan pemrosesan data pribadi, maka Perusahaan Pers adalah pengendali data pribadi.	
7.	**Menentukan dasar pemrosesan data pribadi yang sesuai untuk digunakan perusahaan** 7.1. UU PDP secara garis besar memberikan pengendali data pribadi pilihan dasar pemrosesan data pribadi baik atas dasar persetujuan, perjanjian, pemenuhan kewajiban hukum, pelindungan kepentingan vital, pelaksanaan tugas kepentingan umum, maupun pelaksanaan kepentingan yang sah, tergantung konteks, kebutuhan, dan kondisi pengendali data pribadi. Setiap penggunaan dasar pemrosesan memiliki persyaratan dan kewajiban yang harus dipenuhi, 7.2. Perusahaan Pers, sebagai suatu entitas privat, pada umumnya dapat menggunakan dasar pemrosesan berupa persetujuan, perjanjian, maupun pelaksanaan kepentingan yang sah sebagai dasar pemrosesan data pribadi. Konsekuensi pemilihan dasar hukum tersebut akan terlihat pada dokumen terkait pemrosesan data pribadi yang disiapkan oleh Perusahaan Pers. 7.3. Dalam hal Perusahaan Pers bertindak sebagai prosesor maka dasar pemrosesan data pribadi akan ditentukan oleh pihak yang menjadi Pengendali Data Pribadi.	
8.	**Melakukan *reviu* dokumen, produk, atau keluaran yang berpotensi mengandung data pribadi** Reviu terhadap dokumen atau produk yang telah dipublikasikan oleh Perusahaan Pers perlu dilakukan untuk memahami potensi publikasi data pribadi, sebagai bagian pemrosesan data pribadi. Pada umumnya, dokumen atau produk yang mengandung data pribadi meliputi pengumuman kegiatan dengan data pribadi subjek data sebagai narahubung, informasi narahubung suatu pengumuman resmi, dan bentuk keluaran lain.	
9.	**Menunjuk Pejabat Pelindungan Data Pribadi** 9.1. UU PDP mewajibkan pengendali dan prosesor menunjuk pejabat pelindungan data pribadi, dalam hal melakukan pemrosesan data pribadi untuk pelayanan publik, kegiatan inti Pengendali Data Pribadi memiliki sifat, ruang lingkup, dan/ atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas Data Pribadi dengan skala besar; dan kegiatan inti Pengendali Data Pribadi terdiri dari pemrosesan Data Pribadi dalam skala besar untuk Data Pribadi yang bersifat spesifik dan/ atau Data Pribadi yang berkaitan dengan tindak pidana. 9.2. Mengingat saat ini Perusahaan Pers memproses data konsumen dan karyawan secara sistematis, dan dapat dikualifikasikan sebagai pemrosesan data pribadi dengan skala besar (mengingat hingga kini belum ada kriteria spesifik tentang skala besar), maka Perusahaan Pers wajib untuk menunjuk Pejabat Pelindungan Data Pribadi. 9.3. Pejabat Pelindungan Data Pribadi secara umum bertugas memantau dan memastikan kepatuhan Pengendali dan Prosesor dalam kegiatan pemrosesan data pribadi. Perlu diingat Pejabat Pelindungan Data Pribadi tidak secara langsung melakukan kegiatan pemrosesan data pribadi, namun hanya memastikan kepatuhan pihak, unit atau individu yang terlibat dalam pemrosesan data pribadi pengendali atau prosesor	

	melaksanakan kewajiban sesuai peraturan perundang – undangan. 9.4. UU PDP mensyaratkan Pejabat Pelindungan Data Pribadi untuk ditunjuk berdasarkan profesionalitas, pengetahuan mengenai hukum, praktik Pelindungan Data Pribadi, dan kemampuan untuk memenuhi tugas-tugasnya. Hingga saat dokumen ini selesai disusun, belum terdapat sertifikasi resmi dari lembaga manapun untuk pelatihan pejabat pelindungan data pribadi yang diakui oleh Pemerintah.	
10.	**Menyiapkan Kebijakan Privasi *(Privacy Notice)* Bagi Subjek Data** 10.1. Secara spesifik, UU PDP memang belum mensyaratkan kewajiban penyiapan kebijakan privasi. Namun kewajiban pemberitahuan pemrosesan data pribadi turut diatur pada PP PSTE yang berlaku kepada seluruh sistem elektronik, termasuk di antaranya para pengendali dan proses data pribadi. Pada praktiknya, pengendali dan prosesor data pribadi juga menginformasikan kegiatan pemrosesan data pribadi yang dilakukannya kepada subjek data pribadi sebagai bentuk transparansi dan akuntabilitas. 10.2. Dokumen Kebijakan Privasi, diwajibkan menggunakan Bahasa Indonesia, dan paling sedikit berisi informasi: ● Jenis data pribadi, informasi dan relevansi pengumpulan informasi dan data pribadi tersebut, ● Tujuan pemrosesan data pribadi, ● Dasar hukum pemrosesan data pribadi, ● Jangka waktu penyimpanan data pribadi, ● Hak subjek data pribadi, ● Narahubung yang dapat dihubungi, ● Pihak yang terlibat dalam kegiatan pemrosesan data pribadi. ● Ketentuan pembaruan Kebijakan Privasi, ● Kegiatan pemrosesan data pribadi yang dilakukan, dan ● Ketentuan dalam hal terjadi kegagalan pelindungan data pribadi. 10.3. Dokumen ini dapat digunakan untuk memenuhi persyaratan pemrosesan data pribadi konsumen, karyawan, maupun vendor, selama dijelaskan dalam dokumen ini. Selain itu, dokumen ini akan menjadi dasar bagi subjek data pribadi ketika mengajukan upaya hukum atau ganti rugi terkait pemrosesan data pribadi (apabila ada).	
11.	**Menyiapkan Mekanisme Pengumpulan Persetujuan Subjek Data Sebelum Pemrosesan Data Pribadi Dilakukan** 11.1. Sebagai salah satu dasar pemrosesan, persetujuan perlu untuk dikumpulkan oleh Pengendali data pribadi. UU PDP mensyaratkan permintaan persetujuan dilakukan secara *opt-in* dan eksplisit. Hal ini berarti pengendali data harus mendapatkan persetujuan dari subjek data pribadi secara afirmatif, berdasarkan tindakan atau pernyataan yang secara terang menjelaskan persetujuan subjek data pribadi terhadap pemrosesan data pribadi**.** 11.2. Pada praktiknya, akan terdapat metode pengumpulan persetujuan data pribadi yang berbeda, tergantung subjek data pribadi yang memberikan persetujuan. Dalam kegiatan pemrosesan data pribadi oleh Perusahaan Pers, bentuk pengumpulan persetujuan dilakukan sebagai berikut:	

	● Apabila pengumpulan data pribadi dilakukan terhadap karyawan, maka pengumpulan persetujuan karyawan dapat dilaksanakan pada saat penandatanganan perjanjian kerja, selama perjanjian tersebut menyertakan klausa permintaan persetujuan data pribadi. ● Apabila pengumpulan data pribadi dilakukan terhadap konsumen, maka pengumpulan persetujuan konsumen dapat dilaksanakan dengan menyediakan *check-box* yang menyatakan konsumen menyetujui dilakukan pemrosesan data pribadi. Check-box dapat disediakan pada kesempatan pertama sebelum terjadi pemrosesan data pribadi. Biasanya dilakukan sebelum pengumpulan *cookies* melalui penyediaan *cookies wall*, atau sebelum konsumen mendaftar sebagai pengguna/pelanggan suatu layanan. ● Apabila pengumpulan data pribadi dilakukan terhadap vendor, maka pengumpulan persetujuan vendor dapat dilaksanakan pada saat penandatanganan perjanjian kerja, sama, sepanjang perjanjian tersebut menyertakan klausa permintaan persetujuan data pribadi. 11.3. Sebagai bentuk pelaksanaan kewajiban ini secara teknis, pengendali dapat mengalokasikan salah satu database yang dimiliki, dikhususkan untuk menyimpan metadata persetujuan yang direkam secara digital. Paling sedikit, dalam praktiknya, metadata tersebut terdiri dari: *timestamp*, jenis data pribadi yang dikumpulkan/proses, tujuan, *user identifier* (seperti *user ID*), status *consent*, dan kalimat persetujuan/*consent statement*.	
12.	**Menyusun Kebijakan Internal Pemrosesan Data Pribadi** 12.1. Secara spesifik, UU PDP memang belum mensyaratkan kewajiban penyiapan kebijakan internal pemrosesan data pribadi. Namun kewajiban untuk memiliki kebijakan tata kelola turut diatur pada PP PSTE yang berlaku kepada seluruh sistem elektronik, termasuk di antaranya para pengendali dan proses data pribadi. UU PDP sendiri mensyaratkan pengendali menyusun dan menerapkan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan. 12.2. Pada praktiknya, pengendali dan prosesor data pribadi menyusun kebijakan internal pemrosesan data pribadi sebagai bagian dari kebijakan pengelolaan informasi dan/atau sistem elektronik dalam perusahaannya. 12.3. Kebijakan Internal Dokumen tersebut meliputi, antara lain, sebagai berikut: ● aspek-aspek privasi dalam kegiatan pemrosesan data pribadi oleh Perusahaan Pers, baik *privacy by design* dan *privacy by default* dalam pengembangan perangkat lunak atau *software development lifecycle;* ● jenis dan ragam data pribadi yang diproses oleh Perusahaan Pers; ● pembagian tanggung jawab pihak internal dalam pemrosesan data pribadi; ● kewajiban Perusahaan Pers kepada subjek data pribadi; ● mekanisme penanganan pelaksanaan hak subjek data pribadi; ● ketentuan respon dalam hal terjadi kegagalan pelindungan data pribadi; ● ketentuan pelibatan pihak ketiga dalam pemrosesan data pribadi; ● bentuk kegiatan pemrosesan data pribadi yang dilakukan oleh organisasi; ● jangka waktu penyimpanan data pribadi; ● larangan serta kewajiban individu yang terlibat dalam pemrosesan data pribadi;	

	● pemrosesan data pribadi yang diterima dari selain subjek data; ● mekanisme pengiriman data pribadi ke pihak lain di dalam dan luar negeri; ● mekanisme ketika organisasi melakukan pemisahan, pengambilalihan, peleburan, penggabungan, dan pembubaran badan hukum; ● mekanisme audit, prosedur pengoperasian, tugas, wewenang, dan kontak pejabat pelindungan data pribadi; ● ketentuan klasifikasi informasi (*information classification policy*) yang mengatur segregasi dan klasifikasi data pribadi yang diproses oleh Perusahaan Pers yang dapat dicantumkan dalam kebijakan pelindungan data pribadi serta mendefinisikan bagaimana penanganan dan langkah keamanan yang harus diimplementasikan atas bentuk informasi tertentu; ● ketentuan terkait kriptografi dan enkripsi untuk memastikan keamanan, integritas, dan ketersediaan data pribadi; ● kebijakan terkait keamanan operasional yang mencakup namun tidak terbatas kepada *backup*, *logging and monitoring*, *penetration testing,* keamanan terhadap *malware*, dan *vulnerability management*; ● manajemen keamanan informasi dan insiden keamanan informasi yang mencakup proses dan peran dan tanggung jawab karyawan dalam hal terjadi insiden keamanan; dan ● Ketentuan terkait *Business Continuity* dan *Disaster Recovery* yang mencakup keberlangsungan bisnis dalam hal terjadi bencana alam dan/atau kondisi lain serupa.	
13.	**Menyiapkan Data Protection Impact Assessment** 13.1. UU PDP mensyaratkan pengendali untuk melakukan *Data Protection Impact Assessment (DPIA)* atau penilaian dampak pemrosesan data pribadi yang memiliki risiko tinggi, meliputi pengambilan keputusan secara otomatis yang memiliki akibat hukum atau dampak yang signifikan terhadap Subjek Data Pribadi, pemrosesan atas Data Pribadi yang bersifat spesifik, pemrosesan Data Pribadi dalam skala besar, pemrosesan Data Pribadi untuk kegiatan evaluasi, penskoran, atau pemantauan yang sistematis terhadap Subjek Data Pribadi, pemrosesan Data Pribadi untuk kegiatan pencocokan atau penggabungan sekelompok data, penggunaan teknologi baru dalam pemrosesan Data Pribadi, dan/ atau, pemrosesan Data Pribadi yang membatasi pelaksanaan hak Subjek Data Pribadi. 13.2. UU PDP sendiri belum secara spesifik mengatur kriteria tentang DPIA, namun merujuk pada praktik industri, serta RPP UU PDP, kriteria DPIA sebagai berikut: ● deskripsi secara sistematis mengenai kegiatan pemrosesan Data Pribadi dan tujuan pemrosesan Data Pribadi, termasuk kepentingan dari Pengendali Data Pribadi dari pemrosesan ini; ● penilaian kebutuhan dan proporsionalitas antara tujuan dan kegiatan pemrosesan Data Pribadi; ● penilaian risiko terhadap pelindungan hak Subjek Data Pribadi; dan ● langkah yang digunakan Pengendali Data Pribadi untuk melindungi Subjek Data Pribadi dari risiko pemrosesan Data Pribadi.	
14.	**Menyiapkan Data *Transfer Impact Assessment***	

	14.1. UU PDP mensyaratkan pengendali data melakukan *data transfer impact assessment* atau penilaian atas setiap kegiatan pengiriman data pribadi ke pihak ketiga (baik di dalam negeri maupun di luar negeri) dalam bentuk penilaian efektifitas instrumen hukum yang digunakan sebagai dasar pengiriman data pribadi. 14.2. UU PDP belum mengatur kriteria *Data Transfer Impact Assessment*, namun RPP UU PDP saat ini telah mengatur kriteria efektivitas instrumen hukum yang mensyaratkan pengendali data pribadi untuk mempertimbangkan: ● Dasar regulasi yang digunakan; ● Tujuan transfer dan pemrosesan Data Pribadi; ● Pihak yang terlibat dalam pemrosesan Data Pribadi; ● Lingkup sektor transfer Data Pribadi; ● Kategori Data Pribadi yang ditransfer; ● Pilihan mekanisme transfer Data Pribadi yang digunakan; ● Tempat penyimpanan dan akses terhadap Data Pribadi; ● Format Data Pribadi yang akan ditransfer, misalnya dalam teks biasa/disamarkan atau dienkripsi; ● Kemungkinan Data Pribadi dapat ditransfer lebih lanjut dari negara penerima ke negara lainnya; ● Tindakan penilaian terhadap risiko atau dampak terhadap hak-hak Subjek Data Pribadi akibat transfer Data Pribadi; ● Data Pribadi yang ditransfer cukup, relevan, dan terbatas pada yang diperlukan untuk tujuan transfer Data Pribadi; dan ● Langkah prosedural dan evaluasi terhadap pelaksanaan transfer Data Pribadi	
15.	**Menyiapkan *Legitimate Interest Assessment* (jika diperlukan)** 15.1. UU PDP mensyaratkan pengendali data pribadi untuk melakukan analisis kepentingan yang sah dalam hal pengendali data pribadi menggunakan kepentingan yang sah atau legitimate interest sebagai dasar pemrosesan data pribadi. 15.2. UU PDP belum mengatur kriteria *Legitimate Interest Assessment*, namun RPP UU PDP mengatur bahwa pengendali data pribadi dapat menggunakan kepentingan yang sah sebagai dasar pemrosesan data pribadi apabila: ● telah melakukan analisis terhadap keperluan, tujuan, dan keseimbangan antara hak Subjek Data Pribadi dan kepentingan Pengendali Data Pribadi dengan hasil analisis menunjukkan bahwa Pengendali Data Pribadi memiliki kepentingan yang sah untuk melakukan pemrosesan Data Pribadi; dan ● telah melakukan penilaian bahwa pemrosesan yang menggunakan dasar pemrosesan Data Pribadi pemenuhan kepentingan yang sah lainnya tidak merugikan Subjek Data pribadi dengan hasil Pengendali Data Pribadi memiliki dan telah melakukan langkah untuk mengurangi dampak dari pemrosesan Data Pribadi.	
16.	**Menyiapkan Perekaman Kegiatan Pemrosesan Data Pribadi / *Record of Processing Activities* (RoPA)**	

	16.1. UU PDP mewajibkan pengendali data pribadi untuk melakukan perekaman kegiatan pemrosesan data pribadi/ *Record of Processing Activities* (RoPA). Perekaman ini memiliki fungsi sebagai bentuk inventarisasi kegiatan pemrosesan data pribadi yang dilakukan oleh Pengendali Data Pribadi. 16.2. Namun UU PDP belum menjelaskan kriteria RoPA. RPP UU PDP saat ini telah mengatur ketentuan RoPA, untuk disimpan dalam bentuk tertulis secara elektronik/non-elektronik dan mengandung informasi sebagai berikut: ● nama dan detail kontak Pengendali Data Pribadi, Pengendali Data Pribadi Bersama, dan/atau Prosesor Data Pribadi; ● kontak Pejabat Pelindungan Data Pribadi; ● sumber pengumpulan dan tujuan pengiriman Data Pribadi; ● dasar pemrosesan Data Pribadi; ● tujuan pemrosesan Data Pribadi; ● jenis Data Pribadi; ● kategori Subjek Data Pribadi; ● pihak selain Pengendali Data Pribadi yang dapat mengakses Data Pribadi; ● pemenuhan hak Subjek Data Pribadi; ● pemetaan aliran Data Pribadi; ● masa retensi; dan ● langkah teknis dan organisasi dalam rangka pengamanan Data Pribadi.	
17.	**Menerapkan Fitur – fitur Keamanan Informasi Pada Perangkat dan/atau Instrumen Teknis yang Memproses Data Pribadi** UU PDP mensyaratkan pengendali data pribadi menyusun dan menerapkan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan. Pada praktiknya langkah tersebut dapat dilakukan dalam bentuk sebagai berikut: ● Melakukan enkripsi dan/atau *data masking* atas data pribadi yang diproses dan dikelola oleh Perusahaan pers ● Mengimplementasikan *multifactor authentication* untuk memastikan bahwa karyawan atau personel bersangkutan yang akan mengakses data pribadi ● Memiliki *audit log* atau *trail log* atas aktifitas yang dilakukan oleh karyawan atau personel atas data pribadi (seperti: melihat, menghapus, mereplikasi, dan lainnya), yang direviu setidaknya sekali setahun untuk memastikan bahwa akses terhadap data pribadi diberikan kepada karyawan yang relevan ● Mengimplementasikan *user access matrix* untuk memastikan bahwa hanya karyawan-karyawan tertentu dan berkepentingan saja yang dapat mengakses data pribadi, baik akses secara fisik maupun secara digital. ● Melakukan kontrol atas akses terhadap informasi melalui *user management.* ● Memastikan bahwa metode pengiriman data pribadi yang dipilih merupakan metode pengiriman yang aman, seperti API dengan mengimplementasikan langkah-langkah keamanan yang sesuai (contoh: enkripsi saat data *at-rest* dan *in-transit*). ● Menerapkan keamanan informasi pada setiap fase kepegawaian. Hal ini mencakup verifikasi latar belakang calon karyawan, melakukan pelatihan keamanan informasi,	

	adanya proses disiplin dalam hal terjadi kebocoran data, dan ketentuan keamanan informasi setelah karyawan tersebut tidak lagi menjadi bagian dari perusahaan.	
18.	**Pembuatan Perjanjian Kerjasama dengan Pihak Ketiga** 18.1. Dalam hal pengendali data pribadi bekerja sama dengan pihak ketiga dalam pemrosesan data pribadi, pengendali data perlu menyiapkan perjanjian standar untuk pihak ketiga yang memproses data pribadi dengan menyertakan jaminan pelindungan data pribadi terhadap data pribadi yang disediakan oleh organisasi. Pada praktiknya hal ini dapat berupa kerja sama dengan pihak lain sebagai prosesor, kerja sama untuk pengiriman data, kerja sama pengendalian bersama (*Joint Controller*) atau bentuk kerja sama lainnya. 18.2. Jika posisi Perusahaan Pers sebagai pengendali data pribadi, menggunakan layanan pihak ketiga (misal: *Google Cloud, Microsoft Onedrive*, dsb), dapat dipahami bahwa sulit untuk melakukan pengubahan ketentuan perjanjian. Dalam hal ini, Pengendali Data Pribadi dapat mengupayakan untuk meminta penyedia layanan memberikan pernyataan yang pada intinya memberikan jaminan keamanan dan kesesuaian praktik pemrosesan data pribadi sesuai ketentuan yang berlaku. 18.3. Perusahaan Pers, sebagai pengendali data pribadi, wajib memastikan bahwa pihak ketiga yang melakukan pemrosesan data pribadi atas nama Perusahaan Pers (jika ada) memiliki level keamanan yang mumpuni untuk menjaga kerahasiaan data pribadi. Hal ini dapat dilakukan dengan melakukan pengawasan atas pihak ketiga tersebut, melalui pelaksanaan dan pemantauan pemenuhan ketentuan perjanjian. 18.4. UU PDP hanya mengatur perjanjian dengan prosesor, dimana prosesor wajib mendapatkan persetujuan tertulis dari pengendali data apabila prosesor bermaksud meminta pihak lain melakukan pemrosesan data pribadi (*sub-processing*). Ketentuan perjanjian lebih detil diatur dalam RPP UU PDP.	
19.	**Pemberitahuan Kegagalan Pelindungan Data Pribadi** 19.1. UU PDP mensyaratkan pengendali data pribadi mengirimkan dokumen notifikasi kegagalan pelindungan data pribadi kepada subjek data pribadi dan lembaga PDP yang berisi informasi: ● Data Pribadi yang terungkap; ● Deskripsi jenis kegagalan Pelindungan Data Pribadi; ● Waktu dan cara Data Pribadi terungkap; ● Dampak kegagalan Pelindungan Data Pribadi terhadap Subjek Data Pribadi; ● Upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi; dan ● Informasi narahubung. 19.2. Dalam hal kegagalan Pelindungan Data Pribadi mengganggu pelayanan publik dan/ atau berdampak serius terhadap kepentingan masyarakat, Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan Pelindungan Data Pribadi.	
20.	**Menyediakan Kanal Komunikasi Bagi Pengguna** Perusahan Pers perlu menyediakan kanal komunikasi bagi pengguna jika terdapat keluhan atau kebutuhan pengguna melaksanakan hak sebagai subjek data dalam UU PDP. Kanal	

	komunikasi ini perlu untuk dipublikasikan atau diinformasikan kepada pengguna pada saat data pribadi mulai dikumpulkan. Kanal komunikasi dapat berupa alamat surel khusus, kontak pesan singkat, dan/atau mekanisme sejenis yang memungkinkan pengguna memberikan informasi yang dibutuhkan untuk melaksanakan hak dan/atau keluhan.	
21.	**Melakukan Pelatihan Bagi Individu yang Memproses Data Pribadi** Perusahaan Pers perlu memberikan pelatihan tentang hal-hal yang perlu diperhatikan dalam kegiatan pemrosesan data pribadi bagi individu dan/atau pihak-pihak yang memproses data pribadi. Pelatihan perlu dilakukan untuk memberikan informasi terkait kebijakan internal perusahaan dalam pemrosesan data pribadi, dan beberapa kemampuan teknis untuk mengamankan kegiatan pemrosesan data pribadi dari ancaman keamanan siber. Selain itu, Perusahaan Pers sebagai pengendali data perlu memberikan pemahaman bagi karyawan atau personel terkait pentingnya kerahasiaan data pribadi. Pemahaman ini dapat diperkuat dengan pengenaan kewajiban penandatanganan perjanjian kerahasiaan oleh karyawan yang bertanggung jawab pada pemrosesan data pribadi untuk mencegah adanya pengungkapan data pribadi secara tanpa hak.	
22.	**Evaluasi Berkala Pelaksanaan Kebijakan** 22.1. Sebagai bentuk pemantauan efektivitas pelaksanaan kebijakan, Perusahaan Pers sebagai Pengendali Data Pribadi perlu untuk melakukan evaluasi kebijakan yang dilakukan. Hal ini diperlukan guna memastikan kebijakan yang berlaku dapat merespon kebutuhan pemrosesan data pribadi yang dilakukan oleh pengendali data pribadi. 22.2. Selain itu, Pengendali Data Pribadi juga perlu melakukan evaluasi Sistem, Solusi, Fitur, Software, Teknologi dan Instrumen terkait sejenis yang memproses data pribadi secara berkala, baik melalui pelaksanaan *penetration testing* atas sistem secara berkala, atau tes lain yang serupa.	

*****