



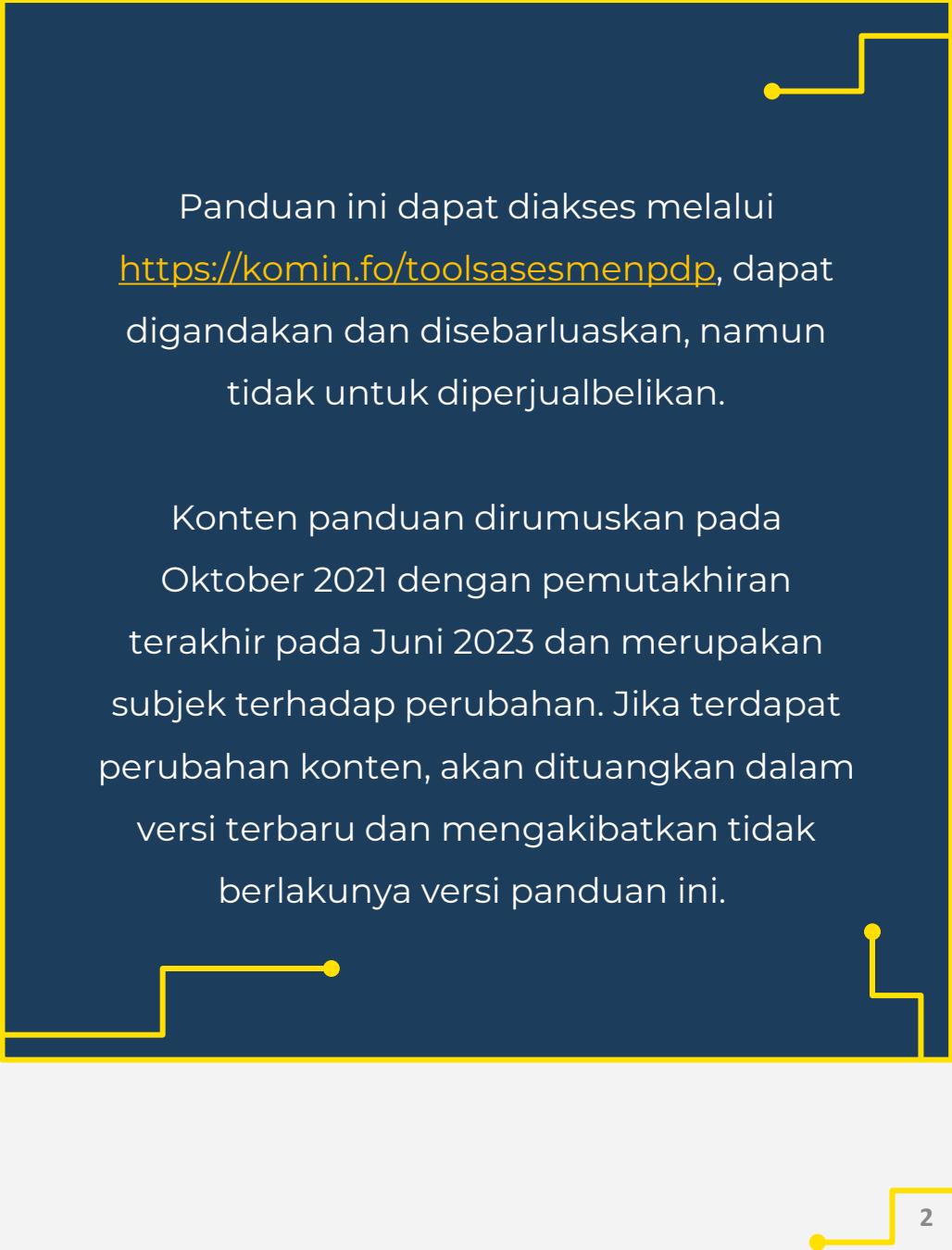
# PANDUAN PENGISIAN

## Tools Asesmen

## Implementasi

## Pelindungan Data Pribadi

Direktorat Pengendalian Aplikasi Informatika  
Direktorat Jenderal Aplikasi Informatika  
Kementerian Komunikasi dan Informatika



Panduan ini dapat diakses melalui  
<https://komin.fo/toolsasesmenpdp>, dapat  
digandakan dan disebarluaskan, namun  
tidak untuk diperjualbelikan.

Konten panduan dirumuskan pada  
Oktober 2021 dengan pemutakhiran  
terakhir pada Juni 2023 dan merupakan  
subjek terhadap perubahan. Jika terdapat  
perubahan konten, akan dituangkan dalam  
versi terbaru dan mengakibatkan tidak  
berlakunya versi panduan ini.

# SISTEMATIKA PANDUAN

<b>DASAR HUKUM</b>	<b>4</b>
<b>PENDAHULUAN</b>	<b>5</b>
<b>DAFTAR ISTILAH</b>	<b>6</b>
<b>PANDUAN PENGISIAN</b>	<b>10</b>
1. Pengumpulan Data Pribadi Secara Terbatas, Spesifik serta Sah Secara Hukum	15
2. Kesesuaian Pemrosesan Data Pribadi dengan Tujuannya	33
3. Jaminan Hak Subjek Data Pribadi	36
4. Keakuratan dan Kelengkapan Pemrosesan Data Pribadi	41
5. Upaya Pengamanan Data Pribadi	44
6. Pemberitahuan Aktifitas Pemrosesan Data Pribadi dan Kegagalan Pelindungan Data Pribadi	60
7. Pemusnahan dan Penghapusan Data Pribadi	68
8. Tanggung Jawab dan Pembuktian Pemrosesan Data Pribadi	74
9. Pengiriman dan Pengungkapan Data Pribadi	82
<b>HASIL ASESMEN IMPLEMENTASI PELINDUNGAN DATA PRIBADI</b>	<b>90</b>
<b>KONTAK TIM PENGAWASAN PDP</b>	<b>94</b>

# DASAR HUKUM

- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah oleh Undang-Undang Nomor 19 Tahun 2016.
- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.
- Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat sebagaimana diubah oleh Peraturan Menteri Komunikasi dan Informatika 10 Tahun 2021.

# PENDAHULUAN

**Tools Asesmen Implementasi Pelindungan Data Pribadi** atau **Tools** adalah alat bantu berbentuk dokumen yang disusun untuk mengetahui tingkat kepatuhan Penyelenggara Sistem Elektronik ("PSE") atau selanjutnya di dalam panduan ini dapat disebut juga sebagai Pengendali dan/atau Prosesor Data Pribadi terhadap ketentuan peraturan perundang-undangan di bidang Pelindungan Data Pribadi (PDP).

PSE, baik Lingkup Publik maupun Lingkup Privat, wajib menyelenggarakan sistem elektronik secara **andal, aman** dan **bertanggung jawab**, serta memenuhi ketentuan Pelindungan Data Pribadi sebagaimana diwajibkan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah oleh Undang-Undang No. 19 Tahun 2016 ("UU ITE"), Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi ("UU PDP"), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ("PP 71/2019"), Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik ("PM 20/2016"), dan Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat sebagaimana diubah oleh Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2021 ("PM 5/2020").

PSE Lingkup Privat meliputi:

- PSE yang diatur atau diawasi oleh K/L berdasarkan ketentuan peraturan perundang-undangan; dan/atau
- PSE yang memiliki portal, situs, atau aplikasi dalam jaringan melalui Internet yang dipergunakan untuk, antara lain, penawaran dan/atau perdagangan barang dan/atau jasa, layanan transaksi keuangan, pengiriman materi atau muatan digital berbayar, layanan komunikasi dalam jaringan dalam bentuk platform digital, layanan jejaring, dan media sosial, layanan mesin pencari, layanan penyediaan informasi elektronik, dan/atau pemrosesan data pribadi.

PSE Lingkup Publik adalah instansi penyelenggara negara atau institusi yang ditunjuk oleh instansi penyelenggara negara.

Seluruh pertanyaan dalam Tools ini disusun berdasarkan kewajiban pemenuhan Pelindungan Data Pribadi dalam PP 71/2019 dan PM Kominfo 20/2016 yang tidak bertentangan dengan UU PDP dan sesuai dengan kewenangan dalam pengawasan yang dilakukan Kementerian Kominfo.

# DAFTAR ISTILAH

<b>Anda</b>	: Pengendali dan/atau Prosesor Data Pribadi yang melakukan pengisian <i>Tools</i> ini.
<b>Penyelenggara Sistem Elektronik (PSE)</b>	: Setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain. Selanjutnya dalam <i>Tools</i> ini dapat disebut juga sebagai Pengendali dan/atau Prosesor Data Pribadi.
<b>Pelindungan Data Pribadi (PDP)</b>	: Keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional Subjek Data Pribadi.
<b>Pengendali Data Pribadi</b>	: Setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.
<b>Prosesor Data Pribadi</b>	: Setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan Data Pribadi atas nama Pengendali Data Pribadi.
<b>Subjek Data Pribadi</b>	: Orang perseorangan yang pada dirinya melekat Data Pribadi.

# DAFTAR ISTILAH

<b>Akses</b>	: Kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan.
<b>Cookies/Internet Cookies</b>	<p>File teks yang disimpan oleh penyedia situs web di komputer pengguna situs web yang dapat diakses kembali oleh penyedia situs web tersebut ketika pengguna mengunjungi situs web pada kesempatan lainnya, yang digunakan untuk memfasilitasi penyelenggaraan Internet atau transaksi, atau untuk mengakses informasi tentang perilaku pengguna.</p>
<b>Dasar Legalitas (<i>lawful bases</i>)</b>	<p>Ketentuan peraturan perundang-undangan yang menjadi dasar syarat sahnya pemrosesan data pribadi, antara lain, adanya persetujuan (<i>consent</i>) dari Subjek Data Pribadi, kewajiban pelaksanaan kontrak hukum yang nyata, pemenuhan kewajiban atau kewenangan hukum, kepentingan yang sah lainnya, dan lainnya. Setiap pihak dilarang memproses data pribadi kecuali memiliki dasar legalitas kegiatan pemrosesannya.</p>
<b>Data Pribadi</b>	: Data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.

# DAFTAR ISTILAH

<b>Data Protection Officer (DPO)</b>	: Pejabat atau Petugas Yang Melaksanakan Fungsi Pelindungan Data Pribadi.
<b>Hak Subjek Data Pribadi</b>	: Hak yang dimiliki Subjek Data Pribadi yang ditetapkan berdasarkan ketentuan peraturan perundang-undangan mengenai pelindungan data pribadi di Indonesia, antara lain, hak mendapatkan informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, hak melengkapi, memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi, hak mendapatkan akses dan memperoleh salinan Data Pribadi, hak untuk mengakhiri pemrosesan, menghapus dan/atau memusnahkan Data Pribadi, hak menarik kembali persetujuan pemrosesan Data Pribadi, hak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis, dan lainnya.
<b>K/L</b>	: Kementerian atau Lembaga.
<b>Kominfo</b>	: Kementerian Komunikasi dan Informatika, khususnya, tim yang bertugas dalam pengawasan pelindungan data pribadi pada Direktorat Pengendalian Aplikasi Informatika.
<b>Korporasi</b>	: Kumpulan orang dan/atau kekayaan yang terorganisasi baik yang berbadan hukum maupun tidak berbadan hukum.

# DAFTAR ISTILAH

<b>Pemrosesan Data Pribadi</b>	: Pemerolehan dan pengumpulan; pengolahan dan panganalisisan; penyimpanan; perbaikan dan pembaruan; penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/atau penghapusan atau pemusnahan.
<b>Pengguna Sistem Elektronik (Pengguna)</b>	: Setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang memanfaatkan barang, jasa, fasilitas, atau informasi yang disediakan oleh PSE
<b>Profiling</b>	: Segala bentuk pemrosesan otomatis data pribadi yang mengevaluasi aspek pribadi Subjek Data Pribadi, khususnya menganalisis atau memprediksi aspek yang berkaitan dengan kinerja orang perseorangan di tempat kerja, situasi ekonomi, kesehatan, preferensi atau minat pribadi, konsistensi tindakan atau perilaku, lokasi atau pergerakan, yang tindakan pemrosesan otomatis tersebut memiliki akibat hukum tertentu atau berdampak secara signifikan bagi Subjek Data Pribadi.
<b>Setiap Orang</b>	: Orang perseorangan atau korporasi.
<b>TDPSE</b>	: Tanda Daftar PSE.
<b>URL Website</b>	: <i>Uniform Resource Locator Website.</i>

**Catatan:**

Sebagian besar istilah yang digunakan dalam *Tools* ini mengikuti UU PDP.

# PANDUAN PENGISIAN

# PANDUAN PENGISIAN

*Tools* dapat diakses melalui <https://komin.fo/toolsasesmenpdp>. Untuk menggunakannya, PSE terlebih dahulu memasukkan informasi mengenai data PSE, gambaran umum sistem elektronik, dan data Petugas PDP/pengisi formulir.

*Tools* menanyakan sejumlah pertanyaan terkait implementasi prinsip-prinsip pemrosesan data pribadi, mengenai pengumpulan data pribadi secara terbatas, spesifik serta sah secara hukum, kesesuaian pemrosesan data pribadi dengan tujuannya, jaminan hak subjek data pribadi, keakuratan dan kelengkapan pemrosesan data pribadi, upaya pengamanan data pribadi, pemberitahuan aktifitas pemrosesan data pribadi dan kegagalan pelindungan data pribadi, pemusnahan dan penghapusan data pribadi, tanggung jawab dan pembuktian pemrosesan data pribadi serta pengiriman dan pengungkapan data pribadi. Apabila Anda membutuhkan penjelasan lebih terkait suatu pertanyaan, di dalam panduan ini memuat penjelasan serta praktik yang baik (*good practices*) dengan contoh praktis yang relevan atas setiap pertanyaan.

Setelah Anda selesai melakukan pengisian, *Tools* secara otomatis akan melakukan perhitungan dan menampilkan laporan hasil pengisian dan saran praktis (atau tingkat lanjut) untuk meningkatkan kepatuhan terhadap ketentuan PDP. Akan tetapi, pemenuhan saran ini atau pengisian *Tools* ini tidak menjamin bahwa kegiatan pemrosesan data pribadi telah memenuhi ketentuan PDP berdasarkan peraturan perundang-undangan. Kami menyarankan Anda untuk berkonsultasi dengan kami atau pihak ketiga lain yang memiliki kompetensi dan kualifikasi yang cukup untuk memberikan advokasi tentang PDP dalam kegiatan pemrosesan data pribadi.

*Tools* tidak dimaksudkan untuk menggantikan atau membebaskan setiap tanggung jawab dan kewajiban yang ditentukan dalam peraturan perundang-undangan, termasuk kewajiban tanggung jawab pengamanan data pribadi dan memiliki DPO. *Tools* ini bertujuan menjadi bahan pertimbangan awal dalam merencanakan dan mengimplementasikan PDP dalam kegiatan pemrosesan data pribadi.

# PANDUAN PENGISIAN

Setiap pertanyaan dalam *Tools* harus Anda jawab dengan jawaban YA atau TIDAK.

Contoh:

*Apakah Anda telah melakukan perekaman terhadap semua kegiatan pemrosesan dalam rangka pelindungan Data Pribadi?*

- Jawab YA jika Anda sudah melakukan praktik perekaman pada semua kegiatan pemrosesan data pribadi.
- Jawab TIDAK jika belum dilakukan.

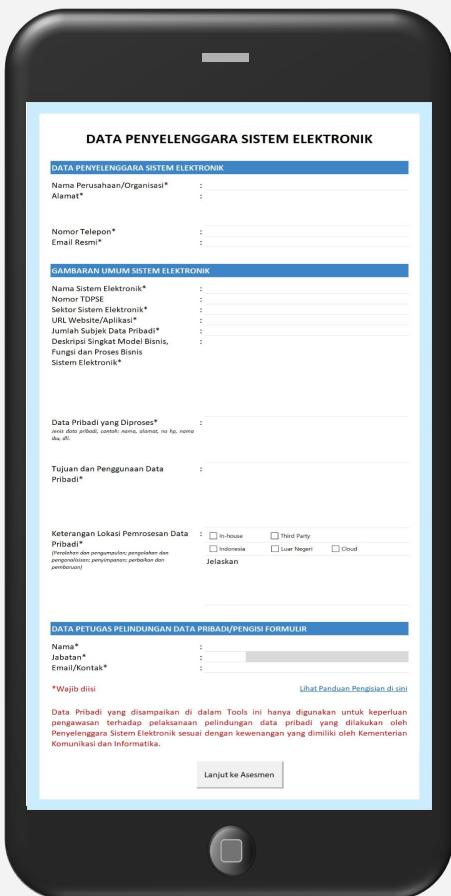
**Pilihan Jawaban YA/TIDAK, yang berarti:**

**YA : ADA PRAKTIK PDP**

**TIDAK : TIDAK ADA PRAKTIK PDP**

**Kami merahasiakan dan melindungi data yang  
Anda isi dalam *Tools* ini.**

# ISIAN IDENTITAS PSE DAN KEGIATAN PEMROSESAN DATA PRIBADI



- PSE mengisi dan menguraikan data serta gambaran umum sistem elektroniknya seakurat dan selengkap mungkin, serta menggunakan data yang terbaru/*update*.
- PSE menyebutkan kegiatan utama bisnis atau layanannya, serta kegiatan penunjang yang memproses data pribadi.
- Data pribadi yang diproses, misalnya data pribadi umum seperti nama, alamat, nomor telepon, *email* atau data pribadi spesifik seperti data anak, data keuangan, data kesehatan, dll.
- Data petugas PDP diisi dengan pejabat/pegawai yang bertanggungjawab atas pelaksanaan PDP, misalnya DPO, *Chief Privacy Officer*, atau pejabat lainnya yang bertanggung jawab atas PDP. Atau bisa juga diisi dengan pejabat/pegawai yang ditugaskan menjadi narahubung dalam hal pelaksanaan PDP.

# ISIAN IDENTITAS PSE DAN KEGIATAN PEMROSESAN DATA PRIBADI

The smartphone screen shows a digital form for Data Subject Processing (PSE) identification and personal data processing activities. The form is divided into several sections:

- DATA PENYELENGGARA SISTEM ELEKTRONIK**
  - Nama Perusahaan/Organisasi\***: PT. XYZ
  - Alamat\***: Jl. MMB No.9 Jakarta
  - Nomor Telepon\***: 123456
  - Email Resmi\***: official@xyz.com
- GAMBARAN UMUM SISTEM ELEKTRONIK**
  - Nama Sistem Elektronik\***: pdpedia
  - Nomor TDPSE\***: 00000x.0x/DIAI/PSE/01/2022
  - Sektor Sistem Elektronik\***: Perdagangan
  - URL Website/Aplikasi\***: pdpedia.com
  - Jumlah Pengguna Aktif**: 500.000
  - Deskripsi Singkat Model Bisnis, Fungsi dan Proses Bisnis Sistem Elektronik\***: pdpedia merupakan marketplace yang dapat digunakan oleh penjual untuk berjualan secara online dengan memasukkan produk beserta harga dan metode pengiriman produk, untuk dibeli oleh customer. Selain itu, pdpedia terintegrasi dengan jasa ekspedisi yang beragam, serta payment gateway.
  - Data Pribadi yang Diproses\***  
Jenis data pribadi, contoh: nama, alamat, no hp, nomer ibu, dll.  
: Nama, jenis kelamin, tanggal lahir, alamat, nomor telepon, alamat email, nomor rekening
  - Tujuan Pemrosesan Data Pribadi\***  
: Data pribadi pengguna diproses untuk pendaftaran pengguna sebagai penjual ataupun pembeli, untuk melakukan transaksi penjualan ataupun pembelian secara online
  - Keterangan Lokasi Pemrosesan Data Pribadi\***  
(Persebaran dan penggunaan pengolahan dan pemrosesan data pribadi; penyimpanan; perbaikan dan penelusuran)
    - In-House
    - Third Party
    - Indonesia
    - Luar Negeri
    - Cloud  
: Pemrosesan data pribadi dilakukan secara terpusat pada Data Center PT. XYZ, yang berlokasi di Jakarta, Indonesia
- DATA PETUGAS PELENDUNGAN DATA PRAWI/PEGISI FORMULIR**
  - Nama\***: Ini Budi
  - Jabatan\***: Lainnya : Direktur Information Technology
  - Email\***: inibudi@xyz.com

\*Wajib diisi

[Lihat Panduan Pengisian di sini](#)

Data Pribadi yang disampaikan tersebut di atas hanya digunakan oleh Kementerian Komunikasi dan Informatika untuk keperluan pengisian Tools Asesmen Implementasi Perlindungan Data Pribadi.

[Lanjut ke Asesmen](#)

## Contoh Pengisian Data PSE

7



## Pengumpulan Data Pribadi Secara Terbatas, Spesifik serta Sah Secara Hukum

## Apakah Pengumpulan Data Pribadi Dilakukan Secara Terbatas dan Spesifik?

Pemrosesan perlu sesedikit mungkin menggunakan data pribadi sepanjang yang hanya dibutuhkan untuk tujuan pemrosesan yang spesifik. Kekurupan data pribadi ditentukan oleh Pengendali Data Pribadi sejauh mungkin berdasarkan kajian atau penilaianya. Data pribadi yang tidak relevan dengan tujuan pemrosesan, tidak perlu dikumpulkan atau dapat dimusnahkan dari kegiatan pemrosesan.

Praktik yang baik:

- Pengendali Data Pribadi melakukan analisis mendalam untuk memeriksa sejauh mana jenis, volume, dan kategori data pribadi yang dibutuhkan untuk mencapai tujuan pemrosesannya. Analisis ini menjawab apakah pengumpulan berbagai macam data pribadi sudah cukup terbatas, spesifik, dan benar-benar diperlukan untuk mencapai tujuan pemrosesannya.
- Dalam hal Pengendali Data Pribadi mengetahui bahwa ada cara atau upaya lain mencapai tujuan pemrosesannya tanpa mengumpulkan data pribadi, maka upaya lain tersebut yang digunakan.
- Pengendali Data Pribadi menentukan variabel dan acuan untuk mengetahui kekurupan data pribadi yang akan diperoleh.
- Pengendali Data Pribadi melakukan verifikasi terhadap setiap tujuan pemrosesannya, khususnya mengetahui tujuan mana saja yang dapat dicapai tanpa melakukan pemrosesan data pribadi. Proses verifikasi ini dilakukan sebelum kegiatan pemrosesan.
- Pengendali Data Pribadi melakukan anomisasi (*anonymization*) atau memusnahkan data pribadi yang tidak relevan dengan tujuan pemrosesannya. Data ini diubah sedemikian rupa sehingga tidak dapat lagi mengidentifikasi Subjek Data Pribadi.
- Apabila diminta otoritas yang berwenang, Pengendali Data Pribadi menunjukkan bahwa setiap data pribadi yang diperoleh sangat relevan dengan tujuan pemrosesannya.

## 1.1

# Apakah Pengumpulan Data Pribadi Dilakukan Secara Terbatas dan Spesifik?

Contoh:

- Penyelenggara *Fintech Lending* membuat daftar debitur bermasalah dan/atau macet yang didalamnya memuat data pribadi debitur. Data pribadi ini hanya terbatas dan spesifik untuk tujuan penagihan tunggakan debitur, antara lain data pribadi tentang nomor kontak, alamat debitur dan jumlah utang jatuh tempo. Penyelenggara *Fintech Lending* menjustifikasi data pribadi yang diproses sudah terbatas dan spesifik untuk memenuhi tujuan pemrosesan data. Setelah tujuan terpenuhi, data pribadi tersebut dimusnahkan oleh Penyelenggara *Fintech Lending* setelah melewati kewajiban jangka waktu retensi data sesuai regulasi.
- Rekrutmen calon pekerja pemantau keamanan sistem elektronik mensyaratkan calon pekerja melengkapi data pribadi yang hanya dibutuhkan untuk tujuan pekerjaan tersebut. Umumnya proses ini tidak membutuhkan data rekam medis karena dapat dijustifikasi tidak relevan dengan tujuan pemrosesan.
- Toko buku *online* mengumpulkan data pribadi pembelinya, antara lain alamat rumah, nomor kontak, dan informasi pembayaran. Akan tetapi, apabila toko ini menjual *e-book* (buku digital), maka alamat pembeli tidak dibutuhkan untuk tujuan pemrosesan ini sehingga Subjek Data Pribadi tidak perlu diminta mengisi alamat rumahnya.

## 1.2

### Dasar Legalitas Apa yang Anda Gunakan untuk Memproses Data Pribadi?

Pemrosesan data pribadi yang dilakukan oleh Pengendali Data Pribadi wajib memiliki legalitas atau dasar pemrosesan data pribadi agar pemrosesan yang dilakukan dapat sah secara hukum.

Sah secara hukum artinya pemrosesan data pribadi dilakukan sesuai dengan ketentuan peraturan perundang-undangan, khususnya menggunakan dasar legalitas pemrosesan. Pengendali data konsisten menerapkan dasar legalitas tersebut terhadap kegiatan pemrosesannya.

Dasar pemrosesan data pribadi tersebut meliputi:

- persetujuan yang sah secara eksplisit dari Subjek Data Pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan oleh Pengendali Data Pribadi kepada Subjek Data Pribadi;
- pemenuhan kewajiban perjanjian dalam hal Subjek Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Subjek Data Pribadi pada saat akan melakukan perjanjian;
- pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;
- pemenuhan pelindungan kepentingan vital Subjek Data Pribadi;
- pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengendali Data Pribadi berdasarkan peraturan perundang-undangan; dan/atau
- pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan Pengendali Data Pribadi dan hak Subjek Data Pribadi.

## 1.2.a

### Persetujuan

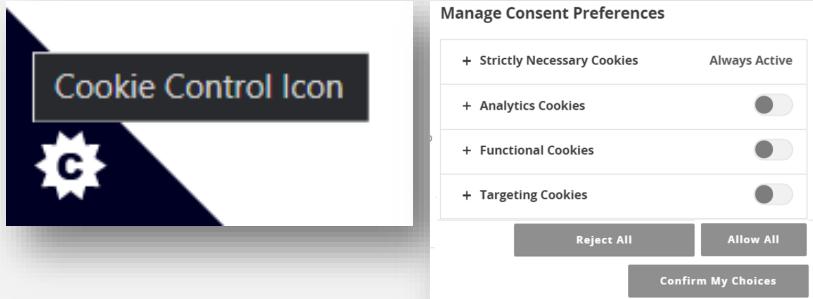
Pemrosesan data harus memenuhi ketentuan adanya persetujuan yang sah dari Subjek Data Pribadi untuk satu atau beberapa tujuan tertentu yang telah disampaikan kepada Subjek Data Pribadi.

Praktik yang baik:

- Persetujuan yang sah adalah persetujuan yang disampaikan secara eksplisit, tidak boleh secara tersembunyi atau atas dasar kekhilafan, kelalaian atau paksaan.
- Persetujuan diminta terlebih dahulu/disertai dengan informasi maksud dan tujuan pemrosesan yang bersifat spesifik dan jelas (*informed consent*).
- Persetujuan disampaikan langsung dan secara aktif (seperti *meng-click checkbox*) oleh Subjek Data Pribadi (bukan persetujuan diam-diam, otomatis, *preselected tick* atau *pre-checked checkbox*).
- Informasi yang menyertai persetujuan dibuat tidak ambigu dan sejalan dengan pengharapan Subjek Data Pribadi secara wajar.
- Persetujuan dapat ditarik kembali oleh Subjek Data Pribadi, kecuali diatur berbeda dalam regulasi PDP.
- Menampilkan formulir persetujuan secara terpisah dan tidak dipadukan dengan formulir/pernyataan lainnya.

## 1.2.a

### Persetujuan



Contoh:

- Pengendali Data Pribadi menampilkan jendela *pop-up* pada aplikasi/halaman webnya untuk meminta persetujuan dari Subjek Data Pribadi/pengguna serta menyampaikan informasi tujuan dan kegiatan pemrosesannya. Jendela *pop-up* tersebut memuat opsi Ya dan Tidak dalam bentuk *check boxes* dan dengan jelas tertulis bahwa 'saya memberikan persetujuan atas pemrosesan data pribadi tentang diri saya' atau 'saya mengerti bahwa data pribadi saya diproses' atau ekspresi sejenis lainnya.
- Persetujuan ambigu: menggunakan *Internet Cookies* yang terinstal dalam perangkat Pengguna dan digunakan oleh Pengendali Data Pribadi sebagai dasar persetujuan seterusnya dari Subjek Data Pribadi.
- Persetujuan yang tidak sah: persetujuan yang disampaikan secara tersembunyi (*silence*), *pre-ticked boxes*, atau nonaktif (*inactivity*).
- Pengendali Data Pribadi memasang *browser plugin/extension* atau sejenisnya yang juga mengumpulkan data pribadi pengguna (seperti *IP Address*), Pengendali Data Pribadi meminta persetujuan dari Subjek Data Pribadi dan juga menyampaikan beroperasinya *plugin* tersebut kepada pengguna.
- Penyediaan permainan interaktif elektronik memastikan penggunanya yang berada di bawah umur telah mendapatkan persetujuan dari orang tua atau walinya untuk menggunakan layanannya.
- Pengendali Data Pribadi melakukan audit atau pemeriksaan *Internet Cookies* secara berkala (*cookies audit*) untuk mengetahui kepatuhannya terhadap ketentuan PDP, khususnya keterpenuhan adanya persetujuan yang sah dari Subjek Data Pribadi.

## 1.2.b

### Kewajiban Perjanjian

Layanan Pengendali Data Pribadi hanya mungkin diselesaikan/diberikan kepada pelanggan jika pelanggan/Subjek Data Pribadi tersebut harus mengadakan kontrak/perjanjian dengan Pengendali Data Pribadi (contoh, layanan hotel untuk mengetahui identitas pemesan, layanan e-commerce untuk mendapatkan alamat pengiriman, dan pembelian tiket perjalanan untuk identitas pemilik tiket, dan sebagainya). Dalam hal pemrosesan data dapat dilakukan tanpa adanya kontrak/perjanjian, maka pemrosesan data tidak dapat berdasarkan pada kontrak/perjanjian, tapi menggunakan dasar legalitas pemrosesan lainnya. Dasar pemrosesan ini tidak berlaku kepada situasi di mana tujuan pemrosesan bermanfaat bagi Subjek Data Pribadi (*useful but not objectively necessary*), tetapi harus benar-benar pengumpulan data pribadi adalah bagian esensial (integral) dengan pemenuhan suatu kontrak.

Praktik yang baik:

- Pengendali Data Pribadi melakukan kajian/analisa untuk memastikan bahwa hanya dengan mengadakan perjanjian, maka layanannya dapat diberikan kepada pelanggan/Subjek Data Pribadi (layanan hotel dan e-commerce – *objectively necessary for the performance of the contract*). Pertanyaan untuk membantu menentukan: Apakah sifat dasar layanan Pengendali Data Pribadi? Apa yang mendasari perlu adanya kontrak? Apa ketentuan pokok dalam kontrak? Apakah kebutuhan adanya kontrak juga sejalan dengan pengharapan Subjek Data Pribadi secara wajar?
- Pengendali Data Pribadi menyediakan kontrak dengan bahasa yang mudah mengerti Pengguna dan berkontrak dengan Pengguna yang cakap secara hukum.
- Kontrak menyebutkan tujuan pemrosesan secara spesifik.
- Pengendali Data Pribadi memastikan Subjek Data Pribadi mengetahui isi kontrak sebelum memberikan persetujuannya.

## 1.2.b

### Kewajiban Perjanjian

Contoh:

- Penyedia jasa pembayaran secara digital kepada pengguna, maka jasa pembayaran tersebut tidak dapat dilakukan tanpa ada data pribadi untuk tujuan pembayaran/penagihan biaya sehingga dasar legalitas pemrosesan dapat menggunakan Pemenuhan Perjanjian/Kontrak dengan pengguna.
- Pengendali Data Pribadi yaitu Pelaku usaha perdagangan melalui sistem elektronik (“PMSE”) mensyaratkan memasukkan alamat tempat tinggalnya. Pengendali Data Pribadi tersebut dapat menggunakan kontrak untuk memproses alamat tersebut untuk keperluan pengiriman barang yang dibelinya, walaupun akhirnya dia membatalkan pembelian. Di lain pihak, Pengendali Data Pribadi tidak dapat memakai dasar kontrak untuk menggunakan alamat tersebut dalam pemetaan preferensi pelanggan karena butuh persetujuan lain.
- Pengendali Data Pribadi menyusun profil pelanggan, yaitu kesukaan dan kebiasaan dari pelanggan berdasarkan riwayat pembelian/kunjungannya. Pemenuhan untuk kontrak jual beli (seperti pada contoh sebelumnya) tidak sesuai untuk dijadikan dasar pemrosesan untuk penyusun profil tersebut. Walaupun Pengendali Data Pribadi tersebut menyebutkan dalam kontrak jual beli tersebut perihal penyusunan profil pelanggan, menyebutan tersebut tidak dapat menjadi fakta bahwa Pengendali Data Pribadi memerlukan data pribadi untuk pemenuhan perjanjian. Jika Pengendali Data Pribadi tetap ingin melakukan pemprofilan seperti tersebut, maka Pengendali Data Pribadi perlu mendasarkan pada ketentuan syarat sah pemrosesan data yang lain.

## 1.2.b

### Kewajiban Perjanjian: Perjanjian vs Persetujuan

*Contoh Sederhana Perbedaan Penggunaan Dasar Legalitas antara Kewajiban Perjanjian dengan adanya Persetujuan*

#### Perjanjian

- Pemenuhan kewajiban perjanjian dalam hal Subjek Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Subjek Data Pribadi pada saat akan melakukan perjanjian.
- Dalam perjanjian terdapat pemenuhan *contract warranties* (contoh: jaminan pelaksanaan dari para pihak).
- Contoh: pemberian jasa yang melibatkan data pribadi yang tanpanya layanan tidak dapat diberikan, seperti reservasi hotel *online*. Tanpa pengisian data pribadi atau apabila persetujuan ditarik saat kewajiban pihak hotel menyediakan layanan belum terlaksana, maka kewajiban dalam perjanjian tidak dapat dipenuhi.

#### Persetujuan

- Persetujuan (*Consent*) : dalam hal persetujuan penggunaan data pribadi ditarik, layanan jasa tetap dapat diberikan. Misalnya: opsi personalisasi pada layanan *streaming* musik. Sewaktu pengguna menarik persetujuan, layanan *streaming* tetap dapat berjalan meskipun dengan menghilangkan beberapa fitur yang membutuhkan persetujuan.

*Untuk layanan streaming musik/video seperti contoh di atas, maka dasar legalitas yang digunakan adalah kewajiban adanya persetujuan/consent dari Subjek Data Pribadi. Tidak boleh menggunakan dasar legalitas pemenuhan kewajiban perjanjian sebagai dasar legalitas utama untuk pemrosesan tersebut.*

## 1.2.c

### Kewajiban Hukum berdasarkan Peraturan Perundang-undangan

Pemenuhan kewajiban hukum dari Pengendali Data Pribadi sebagaimana ditugaskan dengan ketentuan peraturan perundang-undangan di Indonesia. Kewajiban hukum yang bersumber dari peraturan asing tidak berlaku sebagai dasar hukum yang sah untuk kegiatan pemrosesan data oleh Pengendali Data Pribadi.

Praktik yang baik:

- Pengendali Data Pribadi sebagai penyedia jasa dalam skema pengadaan pemerintah yang memuat ruang lingkup kegiatan pemrosesan data pribadi atas nama dan untuk kebutuhan pemberi pekerjaan (K/L) dalam rangka tugas penyelenggaraan negara (tugas pelayanan publik).
- Pengendali Data Pribadi sebagai mitra kerja sama pemerintah berdasarkan kontrak untuk melakukan pemrosesan data pribadi sesuai dengan ruang lingkup pekerjaan yang diatur dalam kontrak antara Pengendali Data Pribadi dengan Instansi Penyelenggara Negara.
- Pengendali Data Pribadi menerima penugasan khusus Pemerintah untuk melakukan pelayanan publik tertentu (seperti pelayanan kesehatan, perizinan, keimigrasian, transportasi, logistik, pendataan/sensus, dan sejenisnya) berdasarkan kontrak atau perintah peraturan perundang-undangan yang secara eksplisit menyebut dan menugaskan Pengendali Data Pribadi tersebut.

## 1.2.c

### Kewajiban Hukum berdasarkan Peraturan Perundang-undangan

Contoh:

- BUMN menerima penugasan khusus Pemerintah atau mendapatkan penunjukan langsung dari K/L berdasarkan keputusan pejabat publik untuk mengembangkan, mengoperasikan, dan mengelola Sistem Informasi Satu Data Vaksinasi Covid-19 yang sumber anggaran pelaksanaannya dibebankan pada APBN.
- Penyedia jasa sistem pembayaran atau badan usaha tertentu mendapatkan tugas dari pemerintah sebagai mitra instansi pengelola Penerimaan Negara Bukan Pajak (PNBP) untuk menerima pembayaran dari pelayanan publik yang menjadi obyek PNBP (seperti pembayaran pemesanan nama untuk pendirian perusahaan atau pembayaran permohonan merek dagang melalui bank atau penyedia jasa pembayaran lainnya).

## 1.2.d

### Pelindungan Kepentingan Vital Subjek Data Pribadi

Pemrosesan diperlukan untuk melindungi kepentingan vital Subjek Data Pribadi atau orang perseorangan lainnya (*vital interest*). Kepentingan vital ini harus menyangkut hidup dan matinya seseorang (atau kelangsungan hidupnya) secara langsung. Dasar legalitas ini berlaku pada keadaan darurat (atau gawat darurat) dan hanya digunakan dalam hal dasar legalitas pemrosesan lain tidak dapat diupayakan.

Praktik yang baik:

- Dalam hal Pengendali Data Pribadi menggunakan *vital interest* sebagai dasar legalitas pemrosesannya, maka Pengendali Data Pribadi membuat dokumentasi lengkap yang menjelaskan alasannya menggunakan kepentingan vital tersebut.
- Subjek Data Pribadi dalam keadaan *vital interest* tidak diperlukan lagi untuk memberikan persetujuan (secara fisik atau langsung).
- Apabila diminta oleh otoritas yang berwenang, Pengendali Data Pribadi dapat memberikan dan menunjukkan pertanggungjawaban atas semua kegiatan pemrosesan data yang dilakukan berdasarkan *vital interest* disertai dengan dokumen pendukung yang terkait.
- Pengendali Data Pribadi mengimplementasikan pengamanan akses ekstra terhadap data pribadi yang diproses berdasarkan dasar legalitas *vital interest*, seperti menerapkan metode enkripsi data, kontrol dan pembatasan akses kepada pihak yang tidak memiliki tujuan yang memadai (*need-to-know basis*), dan mengadopsi standar teknis dan tata kelola *industry best practice*.

## 1.2.d

### Pelindungan Kepentingan Vital Subjek Data Pribadi

Contoh:

- Seseorang diantarkan ke IGD karena kecelakaan. Dalam praktiknya, pihak Rumah Sakit akan melakukan segala tindakan medis yang diperlukan untuk menolong orang tersebut, seperti mendapatkan rekam medisnya. Pengendali Data Pribadi langsung melakukan pemrosesan data pribadi atas data keluarga korban untuk dihubungi keadaan darurat tersebut tanpa didasarkan pada persetujuan dari korban/pasien/Subjek Data Pribadi.
- Pemrosesan data rekam medis pasien diatur, antara lain, dalam Peraturan Menteri Kesehatan tentang Rekam Medis. Pemanfaatan rekam medis dapat dipakai sebagai pemeliharaan kesehatan dan pengobatan pasien.
- Pemrosesan data pribadi terhadap data pasien yang tidak sadarkan diri.

## 1.2.e

### Pelaksanaan Tugas dalam Rangka Kepentingan Umum, Pelayanan Publik atau Pelaksanaan Kewenangan Berdasarkan Peraturan Perundang-Undangan

Pelayanan publik untuk kepentingan umum dapat dicermati dari sumber anggaran pelaksanaannya, yaitu bersumber atau melibatkan APBN/APBD maka dapat dimaknai sebagai pelayanan publik. Hal terkait lainnya adalah pelaksanaan pelayanan publik tersebut berasal dari kewenangan Instansi Penyelenggara Negara sesuai ketentuan peraturan perundang-undangan, baik pelayanan publik yang dikenakan pungutan PNBP atau tidak. Adanya peraturan perundang-undangan yang memuat informasi bahwa pelayanan publik tertentu diselenggarakan demi kepentingan umum.

Sedangkan pelaksanaan kewenangan dimaknai sebagai kekuasaan badan atau pejabat pemerintahan (atau Instansi Penyelenggara Negara lainnya) untuk bertindak dalam ranah hukum publik. Kewenangan ini sebagai dasar legalitas pemrosesan wajib berdasarkan peraturan perundang-undangan dan Asas-Asas Umum Pemerintahan yang Baik (AUPB). Kewenangan ini diperoleh melalui atribusi UUD NRI 1945 atau Undang-undang, delegasi dan/atau mandat dari pejabat atau badan yang lebih tinggi.

Praktik yang baik:

- Pengendali Data Pribadi disini adalah badan dan/atau pejabat pemerintahan atau Instansi Penyelenggara Negara yang memiliki kewenangan penggunaan kekuasaan negara. Namun, orang perorangan atau badan hukum dapat ditunjuk/ditugaskan untuk melaksanakan sebagian kewenangan instansi penyelenggara negara berdasarkan kontrak.
- Dalam hal Pengendali Data Pribadi adalah orang perorangan atau badan hukum yang terikat kontrak melaksanakan sebagian kewenangan, maka Pengendali Data Pribadi wajib menyusun dokumentasi kegiatan pemrosesan data pribadi berdasarkan dasar legalitas ini.

## 1.2.e

### Pelaksanaan Tugas dalam Rangka Kepentingan Umum, Pelayanan Publik atau Pelaksanaan Kewenangan Berdasarkan Peraturan Perundang-Undangan

Praktik yang baik (lanjutan):

- Peraturan perundang-undangan yang hanya dapat dijadikan dasar adalah peraturan tertulis yang memuat norma hukum yang mengikat secara umum dan dibentuk atau ditetapkan oleh lembaga negara atau pejabat yang berwenang melalui prosedur yang ditetapkan dalam peraturan perundang-undangan.
- Dasar hukum tersebut adalah instrumen hukum yang berkedudukan lebih tinggi dan secara eksplisit membatasi hak Subjek Data Pribadi. Pembatasan ini dengan maksud semata-mata untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai ketentuan peraturan perundang-undangan.
- Dengan dasar legalitas ini, Pengendali Data Pribadi berwenang menolak segala klaim atau permintaan penolakan pemrosesan data pribadi yang diajukan oleh Subjek Data Pribadi.
- Pengendali Data Pribadi menyusun dokumentasi dan menerapkan pengamanan data sesuai dengan tingkat risiko pemrosesannya yang ditunjukkan dengan hasil penilaian mandiri dan hasil pemeriksaan auditor independen.

## 1.2.e

### Pelaksanaan Tugas dalam Rangka Kepentingan Umum, Pelayanan Publik atau Pelaksanaan Kewenangan Berdasarkan Peraturan Perundang-Undangan

Contoh:

- Pengendali Data Pribadi adalah Instansi Penyelenggara Negara yang kewenangannya ditentukan dalam suatu undang-undang untuk memproseskan data pribadi, antara lain Undang-Undang Administrasi Kependudukan, Undang-Undang Telekomunikasi, Undang-Undang Kesehatan, Undang-Undang Perpajakan dan sebagainya.
- Pengendali Data Pribadi selaku Instansi Penyelenggara Negara mendelegasikan kewenangan kepada Pengendali Data Pribadi yang juga berkedudukan sebagai Instansi Penyelenggara Negara.
- Pengendali Data Pribadi adalah orang perseorangan atau badan hukum yang mendapat tugas berdasarkan kontrak melaksanakan sebagian kewenangan dari Instansi Penyelenggara Negara untuk pelayanan publik.
- Suatu Badan Layanan Umum (BLU) pada Kementerian Keuangan RI, mengolah Data Pribadi penerima beasiswa. Kewenangan BLU dalam memproses Data Pribadi diperoleh dari ketentuan peraturan perundang-undangan tentang BLU, organisasi dan tata kelola BLU, dan prinsip efisiensi dan efektivitas penyelenggaraan pelayanan publik oleh BLU.
- Pengendali Data Pribadi berkontrak dengan Instansi Penyelenggara Negara dalam pengelolaan dan pengendalian data administrasi kependudukan atau data wajib pajak. Jenis data tersebut didapatkan dari semua penduduk (atau warga masyarakat) Indonesia, tanpa terkecuali. Pemrosesan ini termasuk pelayanan publik untuk kepentingan umum.
- Otoritas pengatur dan pengawas sektor jasa keuangan meminta bank atau lembaga jasa keuangan lainnya menyerahkan laporan secara berkala yang dapat memuat informasi tentang debitur bermasalah atau debitur yang memiliki kredit dengan kolektibilitas macet. Pemrosesan ini termasuk pelayanan publik untuk kepentingan umum.
- Suatu Instansi Penyelenggara Negara membuat daftar wajib pajak yang belum melunasi hutang pajak dan daftar dapat disediakan kepada publik. Penyusunan daftar tersebut adalah sah secara hukum sepanjang: (i) berdasarkan peraturan perundang-undangan; (ii) adanya pemenuhan setiap prinsip PDP sebagaimana apabila berlaku. Penyusunan daftar tersebut untuk pengawasan dan penegakan hukum di bidang perpajakan.

## Pemenuhan Kepentingan yang Sah Lainnya

Pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan Pengendali Data Pribadi dan hak Subjek Data Pribadi. Dasar legalitas ini tidak dapat digunakan secara langsung, tapi harus ada pengkajian yang memadai terlebih dahulu (*legitimate interests assessment*) dan hanya untuk keadaan kasuistik. Dasar legal ini tidak untuk kepentingan Pengendali Data Pribadi atau Subjek Data Pribadi yang bersifat spekulatif atau baru terjadi di masa depan, tetapi kepentingan aktual. Kepentingan yang dimaksud ini harus sejalan dengan ketentuan peraturan perundang-undangan di Indonesia (bukan kepentingan yang bersumber dari hukum luar negeri).

Praktik yang baik:

- Sebelum menggunakan dasar legalitas ini, Pengendali Data Pribadi menyusun kajian tentang kepentingan yang sah dimaksud untuk menganalisis pemenuhan terhadap (i) kespesifikasi kepentingan yang sah dan dasar hukumnya (ii) adanya kebutuhan aktual terhadap tujuan pemrosesan data pribadi disertai dengan upaya pelindungan hak Subjek Data Pribadi yang memadai (*balance-of-interest test*); dan (iii) kepentingan yang sah ini bersifat aktual, bukan kepentingan di masa mendatang.
- Penyelenggara negara tidak dapat menggunakan dasar legalitas ini secara langsung, kecuali didasarkan pada dasar hukum yang sah.
- Pengendali Data Pribadi mengedepankan pengharapan pelindungan data yang wajar dari Subjek Data Pribadi (*reasonable expectation*) dalam kegiatan pemrosesan dengan dasar legalitas ini.
- Pengendali Data Pribadi menunjukkan bahwa ia memiliki kepentingan yang sah dan bersifat lebih memaksa untuk dipenuhi sehingga sah secara hukum membatasi hak Subjek Data Pribadi.
- Walaupun Data Pribadi tersedia secara publik, Pengendali Data Pribadi tidak dapat menggunakannya sebagai alasan pemrosesan data yang dilakukan berdasarkan kepentingan yang sah dari Pengendali Data Pribadi.

Praktik yang baik (lanjutan):

-  Dalam hal menggunakan dasar legalitas ini, Pengendali Data Pribadi menerapkan prinsip transparansi pemrosesan data pribadi, menjustifikasi kesesuaian tujuan pemrosesan dibandingkan dengan tujuan awal pemrosesan data pribadi, memberitahukan tujuan kepentingan yang sah kepada Subjek Data Pribadi, dan menghindari adanya kerugian yang nyata kepada Subjek Data Pribadi.

Contoh:

- Pemrosesan Data Pribadi dalam rangka penerapan strategi *anti fraud* (seperti kecurangan, penipuan, penggelapan aset, pembocoran informasi, tindak pidana perbankan) oleh bank atau lembaga jasa keuangan lainnya. Tindakan pemrosesan ini meliputi pencegahan, deteksi, investasi, pelaporan, sanksi, pemantauan, evaluasi dan tindak lanjut.
- Pemrosesan Data Pribadi untuk tujuan *direct marketing*. Akan tetapi Pengendali Data Pribadi wajib menghentikan permintaan pengiriman materi promosi kepada Subjek Data Pribadi yang menyatakan menolak (*unsubscribe*) dengan atau tanpa disertai alasan.
- Pemrosesan Data Pribadi untuk tujuan administrasi bisnis yang dilakukan (atau saling dipertukarkan) oleh perusahaan dengan anak atau induk perusahaannya. Jenis data meliputi data karyawan dan/atau pelanggan.
- Pemrosesan Data Pribadi untuk tujuan pengamanan pemanfaatan jaringan telekomunikasi dan/atau informasi elektronik.
- Pemrosesan Data Pribadi karyawan untuk melihat kinerjanya, yang mana hal ini merupakan kepentingan yang sah dari pengusaha khususnya membayar upah kepada pekerja sesuai dengan kesepakatan yang ditetapkan berdasarkan satuan waktu dan/atau hasil (capaian). Pengendali Data Pribadi tetap perlu memastikan pemrosesan tersebut tidak menghalangi hak karyawan.
- Tujuan pemrosesan yang perlu dilakukan pengkajian kasuistik: kebebasan pers, menyatakan pendapat di muka umum, kampanye politik atau sosial, mengajukan gugatan hukum/penyelesaian sengketa di luar pengadilan, pelindungan keselamatan dan kesehatan kerja, *whistleblowing system*, tujuan statistik, riset/penelitian ilmiah (*market research*).

2



## Kesesuaian Pemrosesan Data Pribadi dengan Tujuannya

## Apakah Pemrosesan Data Pribadi yang Anda Lakukan telah sesuai dengan Tujuan Pemrosesannya?

Tujuan pemrosesan data pribadi menentukan apa saja data pribadi yang dibutuhkan untuk memenuhi tujuan tersebut. Apabila ditentukan tujuan pemrosesan lanjutan, maka tujuan ini tetap harus sesuai dengan tujuan awal saat data pribadi dikumpulkan.

Apakah Pemrosesan Data Pribadi yang Anda Lakukan telah sesuai dengan Tujuan Pemrosesannya?

Praktik yang baik:

- Pengendali Data Pribadi melakukan *review* secara berkala untuk mengetahui apakah kegiatan pemrosesannya (pengumpulan) data pribadi telah atau masih sesuai dengan tujuan pemrosesannya.
- Pengendali Data Pribadi menganalisis kesesuaian tujuan awal pengumpulan data pribadi dengan tujuan lanjutannya, antara lain, kaitan/hubungan tujuan awal dengan tujuan lanjutannya, ruang lingkup tujuan pemrosesan (termasuk dampak/risiko kepada Subjek Data Pribadi), upaya pengendalian dan pelindungan data tersebut (seperti enkripsi data dan *pseudonymisation*).
- Pengendali Data Pribadi menerima dan mempertimbangkan pendapat/masukan dari Subjek Data Pribadi mengenai apa yang diharapkan dari pemrosesan data pribadi yang dilakukan, serta kelengkapan dan kejelasan dari penjelasan tujuan pengumpulan data pribadi.
- Pengendali Data Pribadi mengubah tujuan pemrosesan lanjutan sesuai dengan harapan yang wajar dari Subjek Data Pribadi mengenai perlindungan dan pemanfaatan datanya, termasuk tindakan meminta persetujuan kembali kepada mereka apabila dasar legalitas tersebut yang berlaku.
- Pengendali Data Pribadi menerapkan kehati-hatian dalam pengungkapan data pribadi kepada pihak ketiga karena pengungkapan ini belum tentu sesuai dengan tujuan pengumpulan data pribadi.

## 2.1

# Apakah Pemrosesan Data Pribadi yang Anda Lakukan telah sesuai dengan Tujuan Pemrosesannya?

Contoh:

- Pengendali Data Pribadi mengumpulkan data pribadi pengguna portal webnya, antara lain, melalui *Internet cookies*. Sebelum pengguna membaca konten portal webnya, Pengendali Data Pribadi menampilkan informasi tentang tujuan penggunaan *cookies* tersebut dan meminta persetujuan kepada Subjek Data Pribadi/pengunjung. *Internet cookies* tersebut kemudian digunakan oleh Pengendali Data Pribadi untuk keperluan yang sama dengan tujuan yang sudah diinformasikan sebelumnya.
- Pengendali Data Pribadi mengungkapkan data pribadi kepada otoritas pengawasan keselamatan dan kesehatan kerja. Tujuan pengungkapan ini masih memenuhi kesesuaian tujuan pemrosesan data pribadi karena didasarkan pada regulasi.
- Pengendali Data Pribadi media sosial daring memberi opsi kepada penggunanya untuk menentukan konten mana saja yang dapat dibaca teman-temannya atau hanya untuk dirinya sendiri. Akan tetapi, pengembang aplikasi pihak ketiga yang berada pada media sosial Pengendali Data Pribadi tersebut masih dapat mengakses konten tersebut walaupun pengguna telah mengatur bahwa konten tertentu hanya untuk dirinya (*only me*). Ini contoh pemrosesan lanjutan yang tidak sejalan dengan tujuan awal Pengendali Data Pribadi tersebut mengumpulkan data pribadi.

3

## Jaminan Hak Subjek Data Pribadi

### 3.1

## Apakah Terdapat Akses atau Kesempatan Bagi Subjek Data Pribadi untuk Melengkapi, Memperbarui dan/atau Memperbaiki Kesalahan dan/atau Ketidakakuratan Data Pribadinya?

Pengendali Data Pribadi wajib memberikan akses atau kesempatan kepada Subjek Data Pribadi untuk melengkapi, memperbarui (*update*), serta memperbaiki kesalahan dan/atau ketidakakuratan data pribadinya tanpa mengganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan. Pengubahan atau pembaruan data berhubungan dengan jaminan akurasi data.

Praktik yang baik:

- Prosedur atau tata cara permintaan pengubahan/pembaruan data pribadi tidak diatur secara spesifik dalam Peraturan Perundang-undangan. Secara praktik, hal ini dapat dilakukan secara lisan maupun tertulis. Sepanjang Subjek Data Pribadi meragukan keakuratan data tersebut dan meminta untuk diganti/diperbarui/diperbaiki, maka Pengendali Data Pribadi dan/atau Prosesor Data Pribadi wajib mengambil langkah-langkah untuk melakukan perbaikan dan melengkapi data.
- Permintaan pemilik data berpotensi eksesif (berlebihan atau di luar kewajaran) jika mengulangi substansi permintaan sebelumnya atau tumpang tindih dengan permintaan lain.

### 3.1

## Apakah Terdapat Akses atau Kesempatan Bagi Subjek Data Pribadi untuk Melengkapi, Memperbarui dan/atau Memperbaiki Kesalahan dan/atau Ketidakakuratan Data Pribadinya?

Contoh:

- Penyedia platform media sosial menyediakan fitur *update* data untuk penggunanya yang ingin memperbarui/memperbaiki data pribadinya.
- Subjek Data Pribadi berkeyakinan data mereka tidak akurat dan berulang kali meminta diganti. Namun Pengendali Data Pribadi telah mengecek dan beranggapan data tersebut akurat. Subjek Data Pribadi terus mengajukan permohonan dengan alasan yang tidak berdasar. Oleh karena itu Pengendali Data Pribadi wajib mengemukakan alasan tidak mengubah data tersebut serta memberikan hak kepada Subjek Data Pribadi untuk menindaklanjuti kepada otoritas yang berwenang.

### Informasi UU PDP:

Pengendali Data Pribadi wajib memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi dalam waktu paling lambat 3x24 jam sejak diterimanya permintaan dari Subjek Data Pribadi. Serta wajib memberitahukan hasil pembaruan/pembetulan tersebut kepada Subjek Data Pribadi.

## 3.2

### Apakah Anda Menyediakan Akses atau Kesempatan bagi Subjek Data Pribadi untuk Memperoleh Salinan Data Pribadi yang Pernah Diserahkan?

Subjek Data Pribadi berhak mendapatkan akses dan salinan historis data pribadi, data yang telah diproses Pengendali dan/atau Prosesor Data Pribadi, maupun data tambahan lainnya (contoh: tujuan pemrosesan data, pihak-pihak yang dapat mengakses data pribadi, berapa lama data tersebut disimpan, informasi keamanan data pribadinya jika ditransfer ke luar negeri, dan lain-lain) sesuai peraturan perundang-undangan yang berlaku.

Praktik yang baik:

- Meskipun permintaan akses data pribadi dapat dilakukan secara lisan, namun praktik terbaik biasanya dilakukan secara tertulis untuk mengantisipasi jika terjadi konflik di kemudian hari.
- Jika Subjek Data Pribadi meminta banyak akses data, maka Pengendali Data Pribadi berhak meminta klarifikasi tentang tujuan permintaan dan memberikan akses data yang relevan sesuai dengan permintaan/tujuan tersebut.
- Data yang diminta dapat diberikan dalam bentuk tertulis, elektronik atau secara lisan.
- Pemberian akses wajib diberikan dalam jangka waktu yang wajar (biasanya 1 bulan sejak permintaan diajukan) dan dapat diperpanjang bergantung pada kompleksitas permintaan data.
- Pengendali Data Pribadi dapat menolak permintaan akses Subjek Data Pribadi dengan memberikan alasan penolakan, memberikan hak kepada Subjek Data Pribadi untuk menempuh jalur lain agar permintaan aksesnya dapat diperoleh.

Contoh:

- Pengendali Data Pribadi menyediakan layanan media sosial berbasis *online* dimana individu dapat bertukar pesan dan gambar. Subjek Data Pribadi meminta salinan data pribadi mereka dan untuk melakukan verifikasi data pribadi apa yang diproses oleh Pengendali Data Pribadi. Pengendali Data Pribadi wajib mengonfirmasi bahwa sedang memproses data pribadi yang berkaitan dengan Subjek Data Pribadi dan memberikan salinannya (seperti nama, detail kontak, pesan, dan gambar yang dipertukarkan). Pengendali Data Pribadi juga wajib memberi informasi tentang pemrosesan – biasanya ada dalam pemberitahuan privasi layanan Pengendali Data Pribadi.

# Informasi UU PDP

## Hak Subjek Data Pribadi dalam UU PDP:

- Mendapatkan Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi
- Melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi tentang dirinya sesuai dengan tujuan pemrosesan Data Pribadi
- Mendapatkan akses dan memperoleh salinan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan
- Mengakhiri pemrosesan, menghapus, dan/atau memusnahkan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan
- Menarik kembali persetujuan pemrosesan Data Pribadi tentang dirinya yang telah diberikan kepada Pengendali Data Pribadi
- Mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis
- Menunda atau membatasi pemrosesan Data Pribadi secara proporsional sesuai dengan tujuan pemrosesan Data Pribadi
- Menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan
- Mendapatkan dan/atau menggunakan Data Pribadi tentang dirinya dari Pengendali Data Pribadi dalam bentuk yang sesuai dengan struktur dan/ atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik
- Menggunakan dan mengirimkan data pribadi tentang dirinya ke Pengendali Data Pribadi lainnya

4

## Keakuratan dan Kelengkapan Pemrosesan Data Pribadi

## 4.1

# Apakah Anda Telah Memastikan Bahwa Data Pribadi Diproses Secara Akurat dan Lengkap?

Pengendali dan Prosesor Data Pribadi wajib memastikan data pribadi diproses secara akurat dan lengkap. Akurat disini maksudnya yaitu data pribadi diambil dan diproses tanpa adanya ketidakakuratan karena kesalahan, kelalaian, kealpaan, dll. Sedangkan lengkap yaitu informasi terkait Subjek Data tidak ada yang dihilangkan.

Praktik yang baik:

- Akurasi data berfokus pada aspek bentuk dan isi data. Kepastian akurasi data dapat dilakukan dengan melakukan audit kualitas data, SDM yang ahli, perbaikan otomatis pada data, dan fokus pada data tertentu untuk diperbaiki, bukan keseluruhan data.
- Untuk menghindari kesesatan data, dapat dilakukan dengan mendokumentasi setiap data, mendokumentasi sumber data, mengambil langkah yang diperlukan untuk memastikan keakuratan data, dan mengidentifikasi berbagai hambatan dalam mendapatkan data yang akurat/ benar.
- Pemutakhiran data dilakukan berdasarkan tujuan pemrosesan data. Jika Pengendali dan/atau Prosesor Data Pribadi membutuhkan data yang mengandalkan kemutakhiran data, maka data harus selalu diperbarui. Namun jika data disimpan hanya untuk keperluan statistik, histori, atau penelitian, maka melakukan pemutakhiran justru merusak tujuan pemrosesan data.

## 4.1

# Apakah Anda Telah Memastikan Bahwa Data Pribadi Diproses Secara Akurat dan Lengkap?

Contoh:

- Ketika mendaftar atau login untuk suatu layanan, penyedia layanan menyediakan fitur verifikasi data menggunakan OTP atau email konfirmasi. Jika data yang diminta terdapat NIK, penyedia layanan juga dapat melakukan verifikasi NIK melalui sistem Dukcapil.
- Di Indonesia, tanggal menggunakan format DD/MM/YYYY, sedangkan apabila Pengendali Data Pribadi juga memiliki *database* di EU, format yang digunakan MM/DD/YY. Jika 09/10/2020 diproses datanya, mana yang paling akurat 10 September atau 9 Oktober? Bentuk data dapat menjadi persoalan karena kurangnya standarisasi.
- Berkaitan dengan kemutakhiran data, kesalahan diagnosis medis tetap didokumentasikan karena menjadi bagian dari rekam medis pasien bahkan setelah diagnosis diperbaiki. Hal ini bertujuan menjelaskan riwayat tindakan medis yang diberikan kepada pasien, atau untuk masalah kesehatan lainnya.

5



## Upaya Pengamanan Data Pribadi

## Apakah Anda Memiliki Prosedur dan Mekanisme Keamanan Data Terhadap Pemrosesan Data Pribadi?

Pengamanan data adalah hal utama dalam mencapai kepatuhan terhadap salah satu prinsip PDP. Pengendali dan Prosesor Data Pribadi wajib memiliki dan menjalankan prosedur dan sarana untuk pengamanan data pribadi dalam sistem elektronik yang dikuasai atau dikelolanya berdasarkan atas risiko untuk menghindari gangguan, kegagalan dan kerugian. Gangguan adalah setiap tindakan yang bersifat destruktif yang mengakibatkan sistem elektronik tidak bekerja sebagaimana mestinya. Kegagalan menjadikan fungsi esensial sistem elektronik tidak beroperasi, sedangkan kerugian menimbulkan akibat hukum bagi pemilik data baik secara materiil dan immateriil, antara lain, *identity fraud*, pemalsuan tagihan dan pembayaran, korban penipuan, tercemarnya aib seseorang, tidak terpenuhinya hak asasnya, dan promosi yang intrusif/mengganggu.

Praktik yang baik:

- Pengendali dan Prosesor Data Pribadi menyediakan rekam jejak audit terhadap seluruh kegiatan pemrosesan data pribadi. Rekam jejak ini dapat diminta sewaktu-waktu oleh otoritas yang berwenang.
- Dalam hal terjadi kegagalan/gangguan sistem yang berdampak serius, Pengendali dan Prosesor Data Pribadi wajib mengamankan data pribadi dan segera melaporkan dalam kesempatan pertama kepada otoritas yang berwenang dan segera tanpa menunda-nunda memberitahukan kepada Subjek Data Pribadi atas dampak serius kebocoran data pribadi agar Subjek Data Pribadi dapat mengantisipasi risiko dari peristiwa tersebut.

## 5.1

# Apakah Anda Memiliki Prosedur dan Mekanisme Keamanan Data Terhadap Pemrosesan Data Pribadi?

Praktik yang baik (lanjutan):

- Pengendali dan Prosesor Data Pribadi memasang instrumen pengamanan dan tata kelola untuk menjaga kerahasiaan data pribadi yang wajib dirahasiakan menurut peraturan perundang-undangan.
- Pengendali dan/atau Prosesor Data Pribadi melakukan edukasi keamanan data kepada pengguna/pengelola data pribadi, serta senantiasa memperbarui aplikasi atau instrumen pengamanan sistem setiap waktu (on-going security update).
- Pengendali dan Prosesor Data Pribadi mengadopsi standar teknis dan tata kelola keamanan data pribadi, antara lain, ISO Manajemen Keamanan Informasi, ISO Teknik Keamanan Data, dan industry best practice.
- Pengendali dan Prosesor Data Pribadi melakukan evaluasi pengamanan data secara berkala dan meningkatkan kelayakan keamanan data berbasis pada risiko pemrosesannya.

Contoh:

- Pengendali Data Pribadi melakukan evaluasi untuk menganalisis kategori sistem elektroniknya, yaitu sistem elektronik strategis, tinggi dan rendah menggunakan "format penelitian mandiri kategorisasi sistem elektronik" sebagaimana diatur dalam Peraturan Badan Siber dan Sandi Negara ("BSSN") mengenai sistem pengamanan dalam penyelenggaraan sistem elektronik. Hasil evaluasi ini dilaporkan kepada otoritas tersebut.

## Apakah Anda Memiliki Prosedur dan Mekanisme Keamanan Data Terhadap Pemrosesan Data Pribadi?

Contoh (lanjutan):

- Pengendali dan/atau Prosesor Data Pribadi menyusun dan menerapkan aturan internal pengamanan data, memetakan para penanggung jawabnya, membatasi akses ke data pribadi, mengaudit/memeriksa para vendornya untuk mengetahui kepatuhan pengamanan data, membuat rencana pemulihan bencana dan rencana penanganan kebocoran data, mengadakan kontrak kerahasiaan data dengan para pihak yang mengakses data pribadi, mengikuti pelatihan keamanan data secara berkala, membuat *password* dan proses autentifikasi lain yang lebih aman, membuat rekam-rekam jejak audit (siapa saja yang mengakses dan dapat memodifikasi data pribadi), menerapkan enkripsi data dan anonimisasi, memasang dan memperbarui aplikasi *Internet security/anti-virus*, memonitor dan mengamankan *traffic* jaringan telekomunikasi, membuat rekam cadang elektronik (*backup*) secara berkala, mengamankan *mobile/portable devices*, melakukan *penetration testing*, memastikan keandalan sistem pemusnahan data, dan memasang pengamanan fisik terhadap setiap komponen sistem elektronik.

## 5.2

# Apakah Anda Memiliki Mekanisme Mengenai Tindakan Mitigasi Risiko dalam hal Terjadi Kegagalan dalam Pelindungan Data Pribadi?

Pengendali Data Pribadi dan Prosesor Data Pribadi wajib menerapkan manajemen risiko dan menyediakan sistem pengamanan yang mencakup prosedur, sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian. Yang dimaksud dengan "sistem pencegahan dan penanggulangan" antara lain *antivirus, anti spamming, firewall, intrusion detection, prevention system*, dan/atau pengelolaan sistem manajemen keamanan informasi.

Praktik yang baik:

- Tindakan pencegahan untuk menghindari terjadinya kegagalan dalam pelindungan Data Pribadi setidaknya mencakup kegiatan: (a). meningkatkan kesadaran sumber daya manusia di lingkungannya untuk memberikan pelindungan Data Pribadi dalam Sistem Elektronik yang dikelolanya; dan (b). mengadakan pelatihan pencegahan kegagalan pelindungan Data Pribadi dalam Sistem Elektronik yang dikelolanya bagi sumber daya manusia di lingkungannya.
- Pengendali Data Pribadi dan Prosesor Data Pribadi sebaiknya menerapkan ISO 31000:2018 *Risk Management — Guidelines*.

## 5.2

# Apakah Anda Memiliki Mekanisme Mengenai Tindakan Mitigasi Risiko dalam hal Terjadi Kegagalan dalam Pelindungan Data Pribadi?

Praktik yang baik (lanjutan):



Tindakan-tindakan mitigasi dapat berupa:

- Meminimalkan penyimpanan data pribadi dengan tidak merekamnya;
- Menghapus data pribadi segera setelah tujuan pemrosesan selesai;
- Menjadwalkan penghapusan data pribadi setelah data tersebut diproses dan diaudit;
- Batasan penggunaan data yang telah dikumpulkan untuk tujuan yang sangat spesifik, dengan memaksimalkan pelindungan hukum, organisasi, dan teknis untuk mencegah tujuan penggunaan data secara tidak sah;
- Adanya sistem, implementasi dan sumber daya kenal aduan yang responsif, didukung oleh sanksi yang tegas dan penegakannya. Berbagai masalah harus dianalisis, untuk menyusun langkah-langkah preventif dan mitigasi yang dapat diterima.

Contoh:

- Bank mengenkripsi semua data keuangan pelanggannya setiap saat. Bank mempertimbangkan untuk melakukan enkripsi ketika menilai kemungkinan adanya potensi ancaman terhadap kegagalan pelindungan data pribadi (misalnya, penipuan keuangan atau pencurian identitas).

## Apakah Anda Menggunakan Jasa Pihak Ketiga sebagai Prosesor Data Pribadi dalam Pemrosesan Data Pribadi?

Dalam menyelenggarakan kegiatan pemrosesan data pribadi, Pengendali Data Pribadi dapat melakukan kegiatan pemrosesan sendiri atau menunjuk pihak ketiga untuk melakukan pemrosesan tersebut, atau disebut sebagai Prosesor Data Pribadi. Pemrosesan data pribadi meliputi perolehan dan pengumpulan, pengolahan dan penganalisisan, perbaikan dan pembaruan, penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan, dan/atau penghapusan atau pemusnahan data pribadi. Jika Pengendali Data Pribadi pada Badan Publik menggunakan layanan pihak ketiga, maka wajib melakukan klasifikasi data sesuai risiko yang ditimbulkan.

Praktik yang baik:

- Substansi kontrak antara Pengendali Data Pribadi dan Prosesor Data Pribadi setidaknya memuat: (i) ruang lingkup pemrosesan data yang dirumuskan secara spesifik dan durasi pemrosesan; (ii) sifat dan tujuan pemrosesan; (iii) Jenis data pribadi dan kategori Subjek Data Pribadi (pelanggan, karyawan, mitra kerjasama, vendor, kreditur, dan lain-lain); dan (iv) hak dan kewajiban Pengendali Data Pribadi dan Prosesor Data Pribadi/pihak ketiga lainnya.
- Jika sistem pemrosesan dan jejak audit merupakan tanggung jawab Prosesor Data Pribadi, maka proses jejak audit tersebut harus sesuai dengan standar yang ditetapkan oleh Pengendali Data Pribadi.
- Penunjukan jasa Prosesor Data Pribadi umumnya mempertimbangkan: (i) jaminan pelindungan data yang optimal; (ii) dapat memberikan keyakinan dan kepuasan sistem pemrosesan data kepada Pengendali Data Pribadi, mencakup penilaian risiko kasus per kasus, dengan mempertimbangkan sifat, ruang lingkup, konteks, dan tujuan pemrosesan, serta risiko pelindungan data; (iii) Pengetahuan dan keahlian jasa pihak ketiga (misal keahlian teknis terkait tindakan keamanan; keandalan prosesor; SDM); (iv) sertifikasi.

## Apakah Anda Menggunakan Jasa Pihak Ketiga sebagai Prosesor Data Pribadi dalam Pemrosesan Data Pribadi?

Praktik yang baik (lanjutan):

- Prosesor Data Pribadi hanya memproses data pribadi sepanjang ada instruksi tertulis dari Pengendali Data Pribadi. Prosesor Data Pribadi menjamin dan memastikan setiap pihak/karyawan yang mengakses data pribadi wajib merahasiakan informasi data tersebut. Prosesor Data Pribadi mengadopsi tata kelola dan implementasi keamanan data berdasarkan standar teknis tertentu. Prosesor Data Pribadi dilarang mengalihkan kewajibannya kepada pihak ketiga lain kecuali terlebih dahulu ada persetujuan tertulis dari Pengendali Data Pribadi. Prosesor Data Pribadi wajib bekerjasama dan melaksanakan permintaan Pengendali Data Pribadi terkait pemenuhan hak Subjek Data Pribadi dan pemberitahuan gangguan keamanan data atau sistem.
- Jika terjadi pengakhiran kontrak, berdasarkan kebijakan dari Pengendali Data Pribadi, Prosesor Data Pribadi memusnahkan setiap salinan atau memindahkan data pribadi kepada sistem Pengendali Data Pribadi. Prosesor Data Pribadi wajib menyediakan informasi dan asistensi untuk pengawasan kepatuhan ketentuan PDP dan/atau audit.

Contoh:

- Pengendali Data Pribadi menggunakan jasa perusahaan A untuk mengelola pembayaran gaji karyawannya. Pengendali Data Pribadi memberikan instruksi yang jelas tentang siapa yang harus membayar, berapa jumlahnya, pada tanggal berapa, oleh bank mana, berapa lama data akan disimpan, data apa yang harus diungkapkan kepada otoritas pajak, dan lain-lain. Dalam hal ini, pemrosesan data dilakukan untuk tujuan Pengendali Data Pribadi membayar gaji kepada karyawannya dan Perusahaan A tidak boleh menggunakan data untuk tujuan apa pun. Cara Perusahaan A harus melakukan pemrosesan telah diuraikan dengan jelas dan ketat. Namun Perusahaan A dapat memutuskan hal-hal terperinci tertentu seputar pemrosesan seperti perangkat lunak mana yang akan digunakan, bagaimana mendistribusikan akses dalam organisasinya sendiri, dan lain-lain. Hal ini tidak mengubah perannya sebagai pemroses selama Perusahaan A tidak melampaui kewenangan atau tujuan pemrosesan yang ditentukan oleh Pengendali Data Pribadi.

## 5.4

# Dalam Hal Penggunaan Jasa Pihak Ketiga sebagai Prosesor Data Pribadi, Apakah Anda Memiliki Perjanjian Tertulis yang Berisikan Ketentuan Pelindungan Data Pribadi?

Pengendali Data Pribadi wajib membuat perjanjian tertulis dengan Prosesor Data Pribadi, baik dalam bentuk kontrak atau bentuk lainnya yang diperbolehkan oleh peraturan perundang-undangan. Pemrosesan data pribadi yang dilakukan oleh Prosesor Data Pribadi juga wajib tunduk pada ketentuan peraturan perundang-undangan tentang pelindungan data pribadi.

Praktik yang baik:

- Perjanjian tertulis dapat disusun oleh salah satu pihak, berdasarkan faktor: posisi para pihak dan kedudukannya dalam kontrak, keahlian teknis, serta akses ke jasa hukum advokat. Misalnya, beberapa penyedia jasa cenderung menetapkan syarat dan ketentuan standar, yang mencakup perjanjian pemrosesan data.
- Prosesor Data Pribadi wajib menerapkan langkah-langkah teknis dan organisasi yang sesuai untuk memastikan keamanan data pribadi, termasuk melindungi dari kerusakan atau kehilangan yang tidak disengaja atau melanggar hukum, perubahan, pengungkapan atau akses yang tidak sah.
- Prosesor Data Pribadi wajib membantu Pengendali Data Pribadi untuk mematuhi ketentuan PDP, yang mencakup keamanan pemrosesan data, menginformasikan terhadap gangguan/kebocoran data, dan penilaian terhadap dampak pemrosesan data.
- Pada pengakhiran kontrak, berdasarkan kebijakan dari Pengendali Data Pribadi, Prosesor Data Pribadi wajib menghapus data pribadi yang sudah tidak terpakai untuk memastikan pelindungan terhadap data pribadi.
- Prosesor Data Pribadi wajib memberikan semua informasi yang diperlukan Pengendali Data Pribadi untuk meningkatkan kepatuhan dalam PDP dan Prosesor Data Pribadi terbuka terhadap audit kepatuhan ketentuan PDP yang dilakukan oleh Pengendali Data Pribadi.

## 5.4

# Dalam Hal Penggunaan Jasa Pihak Ketiga sebagai Prosesor Data Pribadi, Apakah Anda Memiliki Perjanjian Tertulis yang Berisikan Ketentuan Pelindungan Data Pribadi?

Contoh:

- Jasa Pihak Ketiga yang menangani periklanan, selama kontrak berlangsung, pihak ketiga tersebut mendapatkan akses ke data pribadi pelanggan, misal, nomor telepon, alamat domisili atau alamat *email*. Dalam kontrak, diperjanjikan bahwa pihak ketiga hanya boleh menggunakan data pribadi pelanggan hanya untuk keperluan periklanan perusahaan tersebut.
- Untuk menghindari kehilangan data, Pengendali Data Pribadi menggunakan jasa penyedia layanan penyimpanan cadangan data. Karena pihak ketiga tersebut memiliki akses ke data yang disimpan, perjanjian tertulis berisi ketentuan pelindungan data pribadi wajib ditandatangani.

## Apakah Anda Memiliki Aturan Internal Terkait Hal Pemrosesan Data Pribadi?

Setiap Pengendali Data Pribadi harus mempunyai aturan internal terkait pelindungan Data Pribadi untuk melaksanakan pemrosesan Data Pribadi yang sesuai dengan ketentuan peraturan perundang-undangan. Aturan internal ini memuat ketentuan yang berlaku sejak pengumpulan sampai pemusnahan data pribadi.

Praktik yang baik:

- Pengendali Data Pribadi memiliki kebijakan pemrosesan data pribadi untuk dapat dipatuhi oleh setiap karyawan perusahaan pada saat melakukan pemrosesan data pribadi. Apabila pemrosesan melibatkan pihak ketiga, maka aturan dan kebijakan pemrosesan wajib disampaikan kepada mereka (*vendor policy*) dan diawasi kepatuhannya oleh Pengendali Data Pribadi.
- Aturan internal yang dimaksud harus mempertimbangkan aspek penerapan teknologi, sumber daya manusia, metode, dan biaya, serta peraturan perundang-undangan yang berlaku.
- Aturan internal pengelolaan data pribadi mengatur paling sedikit tentang:
  - Edukasi kepada seluruh pihak terkait dalam pemrosesan data pribadi yang dilakukan secara berkala. Ruang lingkup edukasi, antara lain, hak, kewajiban, dan tanggung jawab para pihak tersebut, serta prosedur pengajuan komplain.
  - Pejabat yang berwenang dalam pengambilan keputusan terkait pemrosesan data pribadi dan pengiriman data pribadi kepada pihak ketiga atau Subjek Data Pribadi.
  - Persyaratan atau kondisi pemanfaatan data pribadi (contoh harus adanya perintah dari pejabat yang berwenang dari Pengendali Data Pribadi, dan sesuai dengan ketentuan peraturan perundang-undangan).

## Apakah Anda Memiliki Aturan Internal Terkait Hal Pemrosesan Data Pribadi?

Praktik yang baik (lanjutan):

- Aturan internal pengelolaan data pribadi mengatur paling sedikit tentang (lanjutan):

- Upaya pengamanan terhadap akses ke lokasi penyimpanan data dan media penyimpanan data (contoh adanya otorisasi akses masuk dan log akses).
- Tata kelola fitur otomatis untuk akses ke data pribadi yang dipasang oleh Pengendali Data Pribadi, dan pemeriksaan secara berkala atas beroperasinya fitur otomatis tersebut sebagaimana mestinya.
- Kegiatan perekaman pemrosesan data, serta dokumentasi segala bentuk pengungkapan data.

Contoh:

- Suatu kantor hukum memiliki kebijakan pemrosesan data pribadi yang disosialisasikan dan disetujui setiap karyawan pada saat penerimaan pegawai dikarenakan banyaknya aspek pemrosesan data pribadi dalam pelaksanaan pemberian layanan oleh kantor hukum tersebut. Dengan demikian apabila karyawan kantor hukum terkait melakukan pemrosesan data pribadi, karyawan yang bersangkutan telah memahami sifat kerahasiaan dan cara Pengendali Data Pribadi melakukan pemrosesan data pribadi. Kebijakan internal ini berbeda dengan kebijakan privasi yang disampaikan oleh kantor hukum bersangkutan untuk kliennya.
- Pengendali Data Pribadi menyusun aturan internal pemrosesan data pribadi dengan melibatkan unit bisnis yang memproses data, antara lain, *human resources, ethics, marketing, business development, finance, legal, security, risk, governance, and research and development*.
- Pengendali Data Pribadi membentuk tim internal pengawasan dan pengendalian PDP pada perusahaannya (*privacy team*).

## Apakah Anda Melakukan Sosialisasi kepada Seluruh Pegawai mengenai Aturan Internal Terkait Pemrosesan Data Pribadi?

Terkait dengan kewajiban menyusun aturan internal untuk Pengendali Data Pribadi, maka untuk dapat melaksanakan aturan internal dengan baik maka Pengendali Data Pribadi dapat melakukan sosialisasi aturan internal yang dimaksud.

Praktik yang baik:

- Sosialisasi dilakukan secara berkala dan melalui berbagai media agar seluruh pegawai mengetahui bagaimana cara pemrosesan Data Pribadi beserta perubahan-perubahan yang relevan atas aturan internal tersebut.
- Pengendali Data Pribadi menunjuk satu divisi yang bertanggung jawab memastikan kepatuhan terhadap aturan internal dan jalannya sosialisasi kepada seluruh pegawai.

Contoh:

- Pengiriman *email* kepada seluruh pegawai yang dilanjutkan rapat sosialisasi adanya aturan internal pelindungan data pribadi yang dilakukan setiap 6 bulan sekali dan setiap terdapat perubahan terhadap aturan internal yang terkait.
- Pengendali Data Pribadi melakukan sosialisasi aturan internal terkait pengelolaan dan pelindungan data pribadi, antara lain, melalui forum sosialisasi formal maupun informal, seperti diklat PDP (berbayar atau gratis), *online learning*, poster, buku saku, lokakarya, acara kuis/permainan interaktif, slogan, *roadshow*, *newsletters*, komik, *voicemail broadcast*, pamflet, *digital lobby signage*, mengundang narasumber, dan sebagainya. Sosialisasi ini mencakup sanksi, tanggung jawab jika ada karyawan melakukan pelanggaran aturan internal tersebut, mekanisme penilaian kepatuhan yang diterapkan, prosedur penanganan insiden gangguan atau kegagalan PDP, dan lain-lain. Pengendali Data Pribadi mengalokasi anggaran yang memadai untuk kegiatan sosialisasi ini. Penyelenggaraan sosialisasi tersebut didokumentasikan oleh Pengendali Data Pribadi, antara lain, jumlah dan frekuensi aktivitas sosialisasi, jumlah karyawan dan mitra yang berpartisipasi, metode sosialisasi, persentase ketercapaian target sosialisasi, hasil dari sosialisasi, serta jumlah peserta yang membutuhkan sosialisasi lanjutan atau pelatihan khusus.

## Apakah Anda Memiliki Program Internal Terkait Peningkatan Kesadaran Pelindungan Data Pribadi, Seperti Pelatihan, Lokakarya, atau Lainnya?

Dengan adanya aturan internal pelindungan data pribadi dalam entitas Pengendali Data Pribadi, dalam rangka pencegahan kegagalan pelindungan Data Pribadi (misalnya penyebarluasan tanpa izin data pribadi individual), diperlukan pelatihan internal berkala untuk dapat mengingatkan setiap karyawan yang terlibat dalam pemrosesan data pribadi.

Praktik yang baik:

- Pengendali Data Pribadi mengadakan pelatihan internal secara berkala dan berkelanjutan untuk mensosialisasikan dan mengingatkan kembali penerapan kebijakan aturan internal pelindungan data pribadi.
- Pengendali Data Pribadi mengikutsertakan pengenalan aturan internal pelindungan data pribadi pada program perkenalan karyawan baru.
- Pengendali Data Pribadi memfasilitasi atau mengikutsertakan DPO-nya dalam pelatihan peningkatan kesadaran dan/atau keahlian atau kompetensi PDP.
- Pengendali Data Pribadi memfasilitasi atau mengikutsertakan karyawannya dan semua pihak yang terkait dengan pemrosesan data pribadi dalam pelatihan keamanan data dan penanganan insiden keamanan (*cyber security and incident response*).
- Program pelatihan yang akan digunakan perlu dianalisis kelayakan dan kualitas pelatihannya dengan memperhatikan materi muatan dan cara pelatihan, adanya sertifikasi dan ujian pelatihan, status pengakuan lembaga pelatihan tersebut, dan kegiatan pelatihan berskala internasional.

## 5.7

# Apakah Anda Memiliki Program Internal Terkait Peningkatan Kesadaran Pelindungan Data Pribadi, Seperti Pelatihan, Lokakarya, atau Lainnya?

Contoh:

- Sosialisasi aturan internal pelindungan data pribadi dimulai dari *induction program* untuk karyawan baru.
- Pengendali Data Pribadi mengalokasikan anggaran perusahaannya untuk mengikutsertakan karyawannya dalam pelatihan DPO dan/atau pelatihan PDP.
- Pengendali Data Pribadi memilih lembaga pelatihan yang bereputasi internasional dan memiliki ahli yang mumpuni terkait PDP.
- Pengendali Data Pribadi menyelenggarakan pelatihan yang menarik, seperti gamifikasi (*gamification*) atau mengadakan kontes antar rekan untuk memotivasi mereka agar lebih melindungi data pribadinya dan informasi rahasia perusahaan.
- Pengendali Data Pribadi secara berkala mengeluarkan pamflet, poster, audio visual konten, atau media kampanye *awareness-raising* lainnya untuk memperkuat pemahaman pengguna data pribadi atas ketentuan PDP.
- Pengendali Data Pribadi mengajak para vendor dan mitra bisnisnya kegiatan pelatihan implementasi PDP.

# Informasi UU PDP

Pengendali Data Pribadi wajib melakukan penilaian dampak pelindungan data pribadi jika dalam pemrosesan data pribadi yang dilakukannya memiliki satu atau lebih potensi risiko tinggi terhadap Subjek Data Pribadi.

Potensi risiko tinggi tersebut 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
- Pemrosesan Data Pribadi yang membatasi pelaksanaan hak Subjek Data Pribadi.

# 6

## Pemberitahuan Aktifitas Pemrosesan Data Pribadi dan Kegagalan Pelindungan Data Pribadi

## Apakah Anda Telah Memberitahukan Kepada Subjek Data Pribadi mengenai Aktivitas Pemrosesan Data Pribadi?

Pengendali Data Pribadi wajib menyampaikan informasi (*duty to inform*) kepada subjek data pribadi paling sedikit mengenai identitas Pengendali Data Pribadi, legalitas pemrosesan data pribadi, tujuan pemrosesan data pribadi, jenis dan relevansi Data Pribadi yang akan diproses, aktivitas pemrosesan yang dilakukan, serta bentuk tanggung jawab Pengendali Data Pribadi seperti jangka waktu pemrosesan data pribadi, kelaikan atau keamanan sistem elektronik, tata cara penggunaan perangkat (*terms of use*), dan nomor telepon pusat pengaduan. Kewajiban ini dimaksudkan untuk melindungi kepentingan penggunaan sistem elektronik, termasuk Subjek Data Pribadi.

Bentuk informasi ini dapat berupa *privacy policy*, *data protection notice*, *fair processing notice* atau di Indonesia dikenal dengan Kebijakan Privasi.

### Informasi UU PDP:

Dalam UU PDP, Pengendali Data Pribadi dapat melakukan pemrosesan data pribadi melalui pengambilan keputusan yang didasarkan pada pemrosesan secara otomatis, misalnya dengan pemrofilan atau *profiling*. Subjek Data Pribadi mempunyai hak untuk mengajukan keberatan atas tindakan pengambilan keputusan secara otomatis, dan Pengendali Data Pribadi harus mempunyai mekanisme untuk mengakomodir hak Subjek Data Pribadi tersebut.

Pengambilan keputusan secara otomatis yang memiliki akibat hukum atau dampak yang signifikan terhadap Subjek Data Pribadi termasuk pemrosesan Data Pribadi yang memiliki potensi risiko tinggi terhadap Subjek Data Pribadi, dan Pengendali Data Pribadi wajib melakukan penilaian dampak Pelindungan Data Pribadi terhadap pemrosesan memiliki potensi risiko tinggi ini.

## Apakah Anda Telah Memberitahukan Kepada Subjek Data Pribadi mengenai Aktivitas Pemrosesan Data Pribadi?

Praktik yang baik:

- Pengendali Data Pribadi menyampaikan kepada Subjek Data Pribadi atau kuasanya (jika Subjek Data Pribadi adalah anak-anak) pada saat perolehan data pribadi atau mereka mengakses portal web yang terpasang *Internet cookies*. Informasi yang disampaikan dapat dibuat dua versi, yaitu versi pendek/ringkas dan versi panjang dalam kebijakan pribadi.
- Informasi pemrosesan data kepada Subjek Data Pribadi wajib disampaikan oleh Pengendali Data Pribadi secara ringkas, mudah dimengerti, mudah diakses, menggunakan bahasa lugas, dan sejelas mungkin menyesuaikan usia Subjek Data Pribadi (anak-anak dan dewasa).
- Jika Pengendali Data Pribadi mendapatkan data pribadi dari sumber lain (bukan dari Subjek Data Pribadi), maka batas waktu memberi tahu kepada Subjek Data Pribadi adalah satu bulan atau paling lambat saat data pribadi diungkapkan kepada pihak lain.

Contoh:

- Pengendali Data Pribadi mengirim *email* yang berisi tautan Internet ke portal webnya menginformasikan kegiatan pengumpulan dan pemrosesan data pribadi.
- Pengendali Data Pribadi mengirim *email* atas perubahan kebijakan privasinya.
- Pengendali Data Pribadi menempatkan simbol/icon "baca selengkapnya" atas kegiatan pemrosesan. Upaya lain selain icon, adalah, *just-in-time notification, pop-ups, voice alerts, mobile device gesture*.
- Pengendali Data Pribadi menyampaikan tujuan pemrosesan dengan spesifik, contohnya, "Kami menyimpan data histori transaksi pelanggan dan menggunakan sebagai basis rekomendasi produk lain yang menjadi ketertarikan pelanggan", dibandingkan hanya menyampaikan "Kami menggunakan data pribadi pelanggan untuk meningkatkan layanan kami".

## Apakah Anda Memiliki Mekanisme Pemberitahuan secara Tertulis Kepada Subjek Data Pribadi jika Terjadi Kegagalan dalam Pelindungan Data Pribadi?

Kewajiban ini bagian dari implementasi sarana dan prosedur pengamanan data pribadi. Dalam hal terjadi gangguan atau kegagalan PDP dalam sistem elektronik yang dikendalikan Pengendali Data Pribadi yang berdampak serius, maka Pengendali Data Pribadi wajib segera melaporkannya kepada otoritas yang berwenang pada kesempatan pertama dan kepada Subjek Data Pribadi.

Praktik yang baik:

- Dalam hal terjadi kegagalan kerahasiaan data pribadi atau pelindungannya, maka Pengendali Data Pribadi memberitahu kepada Subjek Data Pribadi dengan ketentuan:
  - Menyampaikan penyebab terjadinya gangguan/kegagalan PDP;
  - Menyampaikannya secara elektronik kepada Subjek Data Pribadi sebagaimana mestinya; dan
  - Memastikan pemberitahuan diterima oleh Subjek Data Pribadi.
- ISO/IEC 27040 defines a data breach as: *compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed.*
- Kewajiban pemberitahuan berlaku sejak diketahui (*aware*) adanya kegagalan atau gangguan PDP. Diketahuinya kegagalan bergantung pada keyakinan Pengendali Data Pribadi yang sewajarnya dimengerti ahli (*reasonable degree of certainty*). Hal yang ditekankan utama adalah tindakan Pengendali Data Pribadi menginvestigasi gangguan tersebut.

## Apakah Anda Memiliki Mekanisme Pemberitahuan secara Tertulis Kepada Subjek Data Pribadi jika Terjadi Kegagalan dalam Pelindungan Data Pribadi?

Contoh:

- Kegagalan PDP dapat berupa kehilangan akses secara permanen atau sementara (kecuali *planned system maintenance*), atau data tentang informasi individu yang disimpan dalam perangkat elektronik akibat dari kejadian pencurian data atau gangguan sistem elektronik. Kegagalan juga dapat terjadi jika data pribadi yang dikelola terkena enkripsi oleh *ransomware*, atau kunci dekripsi yang dimiliki Pengendali Data Pribadi tidak berada lagi bawah kendali/kuasanya.
- Akibat dari kegagalan atau gangguan PDP dapat berupa kerugian materil dan immateriil kepada Subjek Data Pribadi: kehilangan kontrol atas data pribadi, membatasi pelaksanaan hak PDP individu, diskriminasi, pencurian identitas atau penipuan, kerugian finansial, mengungkapkan inisial data pribadi yang memungkinkan teridentifikasi pemilik datanya, kerugian reputasi, dan terungkapnya informasi rahasianya yang sebelumnya dilindungi berdasarkan kewajiban rahasia jabatan/profesi. Akibat ini berdampak secara ekonomi dan sosial terhadap Subjek Data Pribadi.
- Pengendali Data Pribadi menganalisis dampak gangguan atau kegagalan PDP kepada Subjek Data Pribadi, dan apabila berdampak serius, segera tanpa menunda-nunda memberitahu kepada Subjek Data Pribadi dan memastikan mereka mendapatkan pemberitahuan tersebut.
- Pengendali Data Pribadi memasang teknologi atau aplikasi yang memonitor (*detect, address, and report*) insiden kegagalan atau gangguan PDP, dan bekerjasama dengan vendor lain untuk mengatasi atau memulihkan dampak dari gangguan tersebut. Pengendali Data Pribadi memiliki dan mengimplementasikan *incident response plan*.

## Apakah Anda Memiliki Mekanisme Pemberitahuan secara Tertulis Kepada Subjek Data Pribadi jika Terjadi Kegagalan dalam Pelindungan Data Pribadi?

### Informasi UU PDP:

Dalam UU PDP, jika terjadi kegagalan PDP, Pengendali Data Pribadi wajib menyampaikan pemberitahuan mengenai kegagalan yang terjadi kepada Subjek Data Pribadi dan lembaga PDP paling lambat 3x24 jam.

Pemberitahuan tersebut, minimal memuat:

- Data pribadi yang terungkap;
- Kapan dan bagaimana data pribadi terungkap; dan
- Upaya penanganan dan pemulihan atas terungkapnya data pribadi oleh pengendali data pribadi

Pengendali Data Pribadi harus memastikan Subjek Data Pribadi menerima pemberitahuan tersebut.

## 6.3

# Apakah Anda Menyediakan Kanal Aduan yang Dapat Digunakan oleh Subjek Data Pribadi untuk Melaporkan Dampak terhadap Kegagalan Pelindungan Data Pribadi?

Pengendali Data Pribadi wajib menjamin ketersediaan sarana dan layanan pengaduan, dengan setidaknya menginformasikan nomor telepon pusat pengaduan kepada Subjek Data Pribadi. Keberadaan berbagai sarana pengaduan merupakan cara untuk mengukur efektivitas sistem pencegahan pelanggaran data pribadi, sekaligus meningkatkan keandalan pelindungan data.

Praktik yang baik:

- Kanal aduan ini dapat digunakan oleh Subjek Data Pribadi, mitra Pengendali Data Pribadi, karyawan, dan pihak-pihak terkait lainnya terkait kegagalan pelindungan data pribadi.
- Subjek Data Pribadi yang melapor wajib bertindak atas dasar itikad baik, jujur, dan tidak merugikan kepentingan pihak ketiga.
- Dalam menerima laporan pengaduan, Pengendali Data Pribadi wajib menjamin kerahasiaan informasi pengaduan dan identitas pengadu.
- Pengendali Data Pribadi sebaiknya memiliki dokumen tata cara pengaduan dan bagaimana merespon pengaduan tersebut, baik aduan yang mengacu pada kegagalan pelindungan di masa lalu, saat ini, maupun potensi kegagalan pelindungan data pribadi di masa depan.
- Seluruh pengaduan wajib mencantumkan setidaknya tanggal, fakta-fakta yang dilaporkan dan perkiraan tanggal kejadian. Pengadu dapat melampirkan berbagai dokumen yang relevan dengan kasus kegagalan pelindungan data pribadi.
- Pengendali Data Pribadi dalam *website* mereka dapat mencantumkan informasi tentang: (1) Bagaimana cara menghubungi Pengendali Data Pribadi; (2) Bagaimana menghubungi Pengendali Data Pribadi secara online; (3) Kanal aduan bagi penyandang disabilitas

## 6.3

# Apakah Anda Menyediakan Kanal Aduan yang Dapat Digunakan oleh Subjek Data Pribadi untuk Melaporkan Dampak terhadap Kegagalan Pelindungan Data Pribadi?

Contoh:

- Pengantar paket/kurir mendistribusikan sejumlah obat kepada beberapa pasien dari Rumah Sakit. Kurir mengirimkan satu set obat ke pasien yang salah (Pasien A). Pasien A menelepon rumah sakit untuk mengadu. Rumah sakit menyadari resep tersebut sebenarnya untuk pasien yang berbeda dengan nama yang sama (Pasien B). Mereka menghubungi kurir yang kemudian menelepon kembali Pasien A, mengumpulkan barang-barang yang belum dibuka dan mengirimkannya kembali ke Pasien B. Pada titik ini, kurir memberi tahu Pasien B tentang kesalahan tersebut. Pasien B kemudian melayangkan keberatan kepada rumah sakit, karena mereka merasa informasi medis dan alamat mereka telah dibagikan secara tidak tepat dengan Pasien A.

7

## Pemusnahan dan Penghapusan Data Pribadi

## Apakah Anda Menyediakan Mekanisme Penghapusan dan Pemusnahan Data Pribadi sesuai dengan Ketentuan Peraturan Perundang-Undangan?

Pengendali Data Pribadi wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Subjek Data Pribadi, yang mencakup (i) penghapusan (*right to erasure*); dan (ii) pengeluaran dari daftar mesin pencari (*right to delisting*). Khusus berkaitan pengeluaran dari daftar mesin pencari perlu dilakukan berdasarkan penetapan pengadilan.

Praktik yang baik:

 Penghapusan (*right to erasure*) terdiri atas Data Pribadi yang: (a) diperoleh dan diproses tanpa persetujuan Subjek Data Pribadi atau tanpa adanya dasar legalitas pemrosesannya; (b) telah ditarik persetujuannya oleh Subjek Data Pribadi; (c) diperoleh dan diproses dengan cara melawan hukum; (d) sudah tidak sesuai lagi dengan tujuan perolehan berdasarkan perjanjian dan/atau ketentuan peraturan perundang-undangan; (e) penggunaannya telah melampaui waktu sesuai dengan perjanjian dan/atau ketentuan peraturan perundang-undangan; dan/atau (f) ditampilkan oleh Pengendali Data Pribadi yang mengakibatkan kerugian bagi Subjek Data Pribadi.

 Pengeluaran dari daftar mesin pencari (*right to delisting*) dilakukan berdasarkan penetapan pengadilan yang dimohonkan orang yang bersangkutan sebagai Subjek Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan. Permohonan wajib memuat: a. identitas pemohon; b. identitas Pengendali Data Pribadi dan/atau alamat Sistem Elektronik; c. Data Pribadi yang tidak relevan di bawah kendali Pengendali Data Pribadi; dan d. alasan permintaan penghapusan.

## Apakah Anda Menyediakan Mekanisme Penghapusan dan Pemusnahan Data Pribadi sesuai dengan Ketentuan Peraturan Perundang-Undangan?

Praktik yang baik (lanjutan):

-  Pengendali Data Pribadi wajib menyediakan mekanisme penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undang.
-  Mekanisme penghapusan setidaknya memuat ketentuan mengenai: (i) penyediaan saluran komunikasi antara Pengendali Data Pribadi dengan Subjek Data Pribadi; (ii) fitur penghapusan data yang tidak relevan yang memungkinkan Subjek Data Pribadi melakukan penghapusan Data Pribadinya; dan (iii) pendataan atas permintaan penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan.
-  Pada Pengendali Data Pribadi lingkup publik, ketentuan mengenai mekanisme penghapusan dapat dibuat oleh K/L terkait setelah berkoordinasi dengan Menteri Kominfo.

Contoh:

- Penyedia aplikasi pinjaman *online* memberikan opsi penghapusan data pada aplikasi untuk memudahkan penggunaan aplikasi mengajukan permintaan penghapusan data.
- Contoh putusan pengadilan terkait *right to delisting* di Indonesia belum dapat ditemukan. Namun, hak ini merupakan hak yang diminta salah satunya oleh artis Kartika Putri saat menyadari fotonya sebelum berhijab masih beredar di Internet.

## Apakah Anda Menyediakan Mekanisme Penghapusan dan Pemusnahan Data Pribadi sesuai dengan Ketentuan Peraturan Perundang-Undangan?

### **Informasi UU PDP:**

Dalam UU PDP Pengendali Data Pribadi memiliki kewajiban untuk menghapus dan memusnahkan data pribadi dalam hal terpenuhi hal sebagai berikut:

#### Kewajiban menghapus data pribadi dalam hal:

- data pribadi tidak lagi diperlukan untuk pencapaian tujuan pemrosesan Data Pribadi;
- Subjek Data Pribadi telah melakukan penarikan kembali persetujuan pemrosesan Data Pribadi;
- terdapat permintaan dari Subjek Data Pribadi; atau
- data pribadi diperoleh dan/atau diproses dengan cara melawan hukum.

#### Kewajiban memusnahkan data pribadi dalam hal:

- telah habis masa retensinya dan berketerangan dimusnahkan berdasarkan jadwal retensi arsip;
- terdapat permintaan dari Subjek Data Pribadi;
- tidak berkaitan dengan penyelesaian proses hukum suatu perkara; dan/ atau
- data pribadi diperoleh dan/ atau diproses dengan cara melawan hukum.

Pengendali Data Pribadi wajib memberitahukan penghapusan dan pemusnahannya tersebut kepada Subjek Data Pribadi.

#### Kewajiban penghapusan dan/atau pemusnahannya dikecualikan untuk:

- kepentingan pertahanan dan keamanan nasional;
- kepentingan proses penegakan hukum;
- kepentingan umum dalam rangka penyelenggaraan negara; atau
- kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara.

Pemrosesan data pribadi dimusnahkan kecuali masih dalam masa retensi sesuai dengan peraturan perundang-undangan. Kebijakan retensi mencantumkan jenis data pribadi belum dimusnahkan oleh Pengendali Data Pribadi, untuk apa Pengendali Data Pribadi menggunakanannya, dan berapa lama Pengendali Data Pribadi bermaksud menyimpannya. Kebijakan ini membantu Pengendali Data Pribadi menetapkan dan mendokumentasikan periode retensi standar untuk bermacam-macam kategori Data Pribadi.

Praktik yang baik:

- Adanya batas waktu penyimpanan data pribadi dan Pengendali Data Pribadi melakukan analisis secara berkala kapan suatu data pribadi tidak lagi dibutuhkan sehingga perlu dimusnahkan.
- Pengendali Data Pribadi lingkup publik menyimpan data pribadi dalam wilayah Indonesia dengan menggunakan layanan penyimpanan sendiri atau milik pihak ketiga yang layanannya yang berkualitas tinggi dan bersertifikasi.
- Pengendali Data Pribadi menyimpan data pribadi yang telah diverifikasi keakuratannya dan disimpan dalam bentuk data terenkripsi.
- Pengendali Data Pribadi menganalisis adanya batas waktu penyimpanan sesuai yang diatur dalam regulasi.
- Setelah tujuan pemrosesan dipenuhi, Pengendali Data Pribadi menyimpan data pribadi yang telah diubah/dibuat anonim sehingga upaya pengamanannya tidak seketar pengamanan data pribadi.
- Pengendali Data Pribadi tidak menyimpan data pribadi melebihi masa retensi penyimpanan data pribadi dan tidak dapat menggunakan alasan bahwa data tersebut mungkin dapat digunakan kembali di kemudian hari sebagai dasar menyimpan data pribadi.
- Pengendali Data Pribadi menyampaikan jangka waktu penyimpanan data pribadi kepada Subjek Data Pribadi pada saat perolehan data pribadi.

## 7.2

# Apakah Anda Memiliki Kebijakan Retensi terkait Penyimpanan Data Pribadi?

Contoh:

- Pengendali Data Pribadi memberikan opsi/fitur penghapusan data pribadi (dalam aplikasi yang disediakannya) kepada pelanggannya dalam hal ia meng-*uninstall* atau menyatakan menghentikan penggunaan layanan yang diberikan Pengendali Data Pribadi.
- Pengendali Data Pribadi tidak dapat menyimpan data pribadi tanpa adanya batas waktu (permanen), kecuali data tersebut dibuat benar-benar anonim. Pengendali Data Pribadi memusnahkan data pribadi pelanggannya yang meminta pemusnahan atau meninggal dunia.
- Pengendali Data Pribadi memusnahkan data pribadi atas calon pelamar kerja yang tidak lolos seleksi/proses rekrutmen setelah masa retensi tertentu berdasarkan peraturan perundang-undangan. Pengendali Data Pribadi menghapus data pribadi dari mantan karyawannya, termasuk data pribadi keluarganya yang telah diungkapkan oleh karyawan.
- Pengendali Data Pribadi menagih utang debitur perseorangan, dan ketiga debitur sudah melunasi hutangnya dan melampai masa retensi berdasarkan peraturan perundang-undangan, data tersebut dimusnahkan.
- Pengendali Data Pribadi menganalisis atau bertanya kepada otoritas atau advokat/konsultan PDP mengenai adanya batasan waktu penyimpanan data pribadi yang diatur dalam peraturan perundang-undangan (*statutory data retention period*).

### **Informasi UU PDP:**

Pengendali Data Pribadi wajib memusnahkan data yang telah habis masa retensinya, kecuali termasuk dalam kondisi yang dikecualikan. Seperti yang sudah dijelaskan pada pertanyaan sebelumnya.

# 8



## Tanggung Jawab dan Pembuktian Pemrosesan Data Pribadi

## Apakah Anda Telah Melakukan Perekaman terhadap Semua Kegiatan Pemrosesan dalam Rangka Pelindungan Data Pribadi?

Pengendali Data Pribadi dan Prosesor Data Pribadi wajib menerapkan rekam jejak audit terhadap seluruh kegiatan Pemrosesan Data Pribadi dalam sistem elektronik yang dikelolanya. Kewajiban ini adalah bagian dari implementasi tata kelola sistem elektronik yang baik dan akuntabel (*IT Governance*). *IT Governance* mencakup proses perencanaan, pengimplementasian, pengoperasian, pemeliharaan, dan perekaman.

Praktik yang baik:

-  Pengendali Data Pribadi dan Prosesor Data Pribadi memiliki mekanisme rekam jejak audit yang meliputi:
- Memelihara *log* transaksi sesuai dengan kebijakan retensi data penyelenggara berdasarkan peraturan perundang-undangan;
  - Memberikan notifikasi kepada konsumen apabila suatu transaksi berhasil dilakukan;
  - Memastikan tersedianya fungsi jejak audit untuk dapat mendeteksi usaha dan/atau terjadinya penyusupan yang harus direview atau dievaluasi secara berkala; dan
  - Dalam hal sistem pemrosesan dan jejak audit merupakan tanggung jawab pihak ketiga, maka proses jejak audit tersebut harus sesuai dengan standar yang ditetapkan oleh Pengendali Data Pribadi.
-  Apabila diminta otoritas yang berwenang, Pengendali Data Pribadi dan Prosesor Data Pribadi memberikan rekam jejak audit untuk keperluan pengawasan, penegakan hukum pidana, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan untuk keperluan mitigasi atau penanganan tanggap darurat (*incident response*) sesuai dengan ketentuan peraturan perundang-undangan.

## 8.1

# Apakah Anda Telah Melakukan Perekaman terhadap Semua Kegiatan Pemrosesan dalam Rangka Pelindungan Data Pribadi?

Contoh:

- Pengendali Data Pribadi menerapkan prosedur dan sarana perekaman terhadap seluruh kegiatan pemrosesan data pribadi yang meliputi: (a) identitas dan kontak Pengendali Data Pribadi; (b) tujuan pemrosesan; (c) deskripsi kategori Subjek Data Pribadi (jika ada) dan jenis Data Pribadi yang diproses; (d) pihak yang menerima pengungkapan data pribadi; (e) kegiatan transfer Data Pribadi ke luar negeri; (f) sarana dan prosedur pemusnahan Data Pribadi; dan (g) prosedur dan sarana pengamanan Data Pribadi.
- Pengendali Data Pribadi menguraikan kegiatan berdasarkan sejumlah pertanyaan: Daftar pertanyaan tersebut, seperti: “Mengapa Anda perlu menggunakan Data Pribadi?”, “Data Pribadi siapa yang Anda kelola?”, “Data Pribadi dan informasi apa saja yang Anda kumpulkan dari mereka?”, “Kepada siapa Anda mengirimkan atau membagikan Data Pribadi tersebut?”, “Berapa lama Anda menyimpan Data Pribadi tersebut?”, “Bagaimana Anda melindungi Data Pribadi tersebut?” “Unit bisnis mana saja yang memproses Data Pribadi dan jenis Data Pribadi apa yang dikumpulkannya?”
- Pengendali Data Pribadi merekam semua dokumen terkait PDP: kebijakan privasi, manual penyimpanan Data Pribadi, dokumen dalam rangka keamanan Data Pribadi, prosedur pemanfaatan Data Pribadi, perjanjian dengan vendor/prosesor Data Pribadi, perjanjian transfer Data Pribadi, dan seterusnya. Informasi dalam setiap dokumen diperbarui secara berkala.

# Apakah Anda Telah Melakukan Perekaman terhadap Semua Kegiatan Pemrosesan dalam Rangka Pelindungan Data Pribadi?

## Contoh Dokumen Pemrosesan (1)

### Contoh Format Perekaman Terhadap Pemrosesan

#### PSE / PENGENDALI DATA PRIBADI

##### Identitas Pengendali

Pejabat atau Petugas yang Melaksanakan Fungsi Data Pribadi (DPO)

##### Perwakilan (Representative)

(pihak – individu atau badan hukum di Indonesia – yang ditunjuk pengendali atau prosesor data secara tertulis untuk mewakili pengendali atau prosesor data terkait kewajibannya masing-masing berdasarkan regulasi PDP.  
Bisa jadi pengendali sendiri )

Nama	Nama	Nama
Alamat	Alamat	Alamat
Email	Email	Email
Telp	Telp	Telp
Organisasi DPO (jika DPO eksternal)		

##### Rincian kegiatan pemrosesan

##### Tujuan pemrosesan data

##### Data Pribadi yang bersifat spesifik

##### Ya/Tidak

[contoh] Tata kelola pengupahan	No pemrosesan	Tanggal pembuatan dokumentasi	Tanggal dokumentasi diperbarui	[Contoh: Manajemen pengupahan, penghitungan besaran upah, perhitungan besaran bagian upah yang dipotong untuk jaminan sosial]	Tidak
[pemrosesan lain]					

##### Deskripsi tindakan pemrosesan

##### Nama tindakan pemrosesan

##### No. pemrosesan

##### Data pembuatan pemrosesan

##### Pembaharuan pemrosesan

##### Tujuan pemrosesan

##### Tujuan utama

##### Tujuan pendukung 1

##### Tujuan pendukung 2

##### Tujuan pendukung 3

##### Tujuan pendukung 4

##### Tujuan pendukung 5

Para Pihak	Nama	Alamat	Negara	No. telp	Email
Pengendali data					
DPO					
Organisasi DPO (jika DPO eksternal)					
Perwakilan					
Pengendali data bersama (joint controllers)					

# Apakah Anda Telah Melakukan Perekaman terhadap Semua Kegiatan Pemrosesan dalam Rangka Pelindungan Data Pribadi?

## Contoh Dokumen Pemrosesan (2)

Kategori dan Elemen data pribadi	Deskripsi	Jangka waktu penyimpanan		
Nama dan inisial (nama lengkap, inisial)				
Karakteristik personal (misalnya, umur, tanggal lahir, jenis kelamin, tinggi, berat badan, status perkawinan, kewarganegaraan, tempat kelahiran, status kewarganegaraan, minat dan hobi, foto wajah, kemampuan bahasa, jumlah anak, dst).				
Identitas anak				
Riwayat kerja (jabatan, alamat kantor, izin kerja, nomor karyawan, dst)				
Riwayat pendidikan (Ijazah, transkrip, kursus)				
Identitas yang dikeluarakan pemerintah (KTP, KK, SIM, Paspor, NPWP, Kartu BPJS)				
Data koneksitas (alamat IP Internet, nomor kontak, nama akun, kata sandi)				
Data perangkat dan lokasi (pergerakan, GPS, rincian data perangkat elektronik)				
[sebut data pribadi yang bersifat umum lainnya]				
Data pribadi yang bersifat spesifik	Deskripsi	Jangka waktu penyimpanan		
Data dan informasi kesehatan (nomor rekam medis, riwayat perawatan medis, nomor asuransi kesehatan atau jiwa, riwayat transaksi perawatan, klaim asuransi kesehatan, foto diagnosis, hasil tes genetik, data kesehatan pasangan, resep obat, riwayat terapi, riwayat pembelian alat kesehatan)				
Data biometrik				
Data genetika				
Catatan kejahatan				
Data anak				
Data keuangan pribadi				
Tingkatan pengamanan	Teknik pengamanan	Detail		
Tindakan pengamanan 1	[contoh: rekam jejak audit, software protection apps, pencadangan data, enkripsi data, kendali akses data, pengendalian oleh prosesor data, sistem pencegahan dan penangulangan lain, seperti anti-virus, anti-spamming, firewall, instrusion detection, prevention system, pengelolaan sistem manajemen keamanan informasi, dan lain-lain]			
Tindakan pengamanan 2				
Tindakan pengamanan 3				
Penerima Data (Recipient)	Kategori Penerima	Detail		
Penerima data 1	[contoh: bagian internal perusahaan yang memproses data yang ditransfer, prosesor, penerima data di luar negeri atau organisasi internasional, institusi atau mitra komersial, ATAU lain-lain spesifikan]			
Kategori subjek data pribadi	Deskripsi	Detail		
Kategori 1	[contoh: karyawan, penyedia jasa internal pelanggan, vendor/pemasok, penyedia jasa, prospek pelanggan, pendaftar, tamu, karyawan vendor, pengunjung, ATAU lain-lain rincikan]			
Kategori 2				
Kategori 3				
Transfer Data Internasional	Penerima	Negara	Dasar Melakukan Transfer	Nama & Tautan Internet ke Dokumen
Penerima data 1			[tentukan pilihan, contoh: tingkatkan PDP yang setara/kesetaraan PDP, perjanjian antar pengendali data, perjanjian internasional, Binding Corporate Rules (jika berlaku), kode perlaku asosiasi, sertifikasi, ketentuan lain (jika ada)]	
Penerima data 2				
Penerima data 3				

## 8.2

# Apakah Anda Memiliki Pegawai/Karyawan atau Pihak yang Ditunjuk secara Khusus Bertanggung Jawab atas Hal-hal yang Terkait dengan Pelindungan Data Pribadi yang Anda Kelola?

Pengendali Data Pribadi yang melakukan pengelolaan data pribadi wajib menyediakan narahubung (*contact person*) yang mudah dihubungi oleh Subjek Data Pribadi terkait pengelolaan Data Pribadinya. Pengendali Data Pribadi perlu menyampaikan kontak narahubung tersebut kepada Subjek Data Pribadi. Selain narahubung PDP tersebut, Pengendali Data Pribadi wajib menyediakan informasi kontak telepon pusat pengaduan kepada pengguna sistem elektronik.

Praktik yang baik:

- Pengendali Data Pribadi mencantumkan nomor kontak yang dapat dihubungi oleh pengguna sistem elektronik pada sistem elektronik yang digunakan.
- Apabila tidak terdapat nomor yang dapat dihubungi, dapat disertakan cara lain untuk dapat mengontak narahubung (*chat, email, e-form*).
- Narahubung PDP berupa DPO atau pejabat/petugas yang melaksanakan fungsi PDP. Istilah lainnya, *chief privacy officer* (CPO), *chief compliance officer* (CCO), dan *chief information officer* (CIO).
- Pemrosesan data untuk pelayanan publik, pemrosesan data pribadi sensitif, atau pemrosesan data pribadi yang secara rutin dan berskala besar (dalam arti jumlah data, jangka waktu, kategori, dan wilayah cakupan pemrosesan) adalah kegiatan utama Pengendali Data Pribadi, maka Pengendali Data Pribadi disarankan memiliki DPO dan mengadakan analisis dampak dan risiko pemrosesannya. Kegiatan/layanan utama Pengendali Data Pribadi artinya aktivitas operasional Pengendali Data Pribadi dalam memberikan layanan utamanya kepada pelanggan, seperti pemberian fasilitas pelayanan kesehatan yang memproses data pribadi pasien.

## 8.2

# Apakah Anda Memiliki Pegawai/Karyawan atau Pihak yang Ditunjuk secara Khusus Bertanggung Jawab atas Hal-hal yang Terkait dengan Pelindungan Data Pribadi yang Anda Kelola?

Praktik yang baik (lanjutan):

- DPO bertugas antara lain (i) menganalisis kepatuhan PSE terhadap ketentuan PDP berdasarkan regulasi; (ii) melakukan manajemen risiko pemrosesan data pribadi, yaitu identifikasi jenis risiko, penilaian, pengukuran, pemantauan, dan pengendaliannya; (iii) melakukan komunikasi dan kerja sama dengan otoritas yang berwenang; (iv) melakukan pengendalian PDP berbasis risiko; dan (v) perekaman pemrosesan data pribadi. DPO memberikan pendapat dan solusi bagaimana mencapai kepatuhan ketentuan PDP berdasarkan keahlian profesional dan independensinya.

Contoh:

- Penyedia aplikasi *marketplace* menyediakan fitur *chat*, *email*, nomor telepon pada aplikasinya untuk dapat dihubungi oleh pengguna aplikasi.
- Pemrosesan data berskala besar adalah penyelenggaraan satu data vaksin, kartu perjalanan angkutan umum, asuransi jiwa dan kesehatan, pemrosesan oleh mesin pencari Internet, pemrosesan oleh operator jasa telekomunikasi, dan sejenisnya.
- Pengendali Data Pribadi mengadakan rekrutmen DPO yang memiliki kompetensi, yaitu memahami hukum dan implementasi PDP, mengerti aspek keamanan data, mengerti aspek-aspek kegiatan pemrosesan, memiliki kemampuan berkomunikasi yang baik, dan miliki komitmen tinggi menyelenggarakan program peningkatan kesadaran PDP serta pengembangan diri.

## Apakah Anda Memiliki Pegawai/Karyawan atau Pihak yang Ditunjuk secara Khusus Bertanggung Jawab atas Hal-hal yang Terkait dengan Pelindungan Data Pribadi yang Anda Kelola?

### Informasi UU PDP:

Pengendali dan Prosesor Data Pribadi wajib menunjuk pejabat/petugas yang melaksanakan fungsi PDP jika memenuhi satu atau lebih ketentuan berikut:

- Melakukan pemrosesan Data Pribadi untuk kepentingan pelayanan publik
- Kegiatan inti yang memiliki sifat, ruang lingkup, dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas Data Pribadi dengan skala besar
- Kegiatan inti yang terdiri dari pemrosesan Data Pribadi dalam skala besar untuk Data Pribadi yang bersifat spesifik dan/atau Data Pribadi yang berkaitan dengan tindak pidana.

Pejabat/petugas yang melaksanakan fungsi PDP memiliki tugas paling sedikit:

- Menginformasikan dan memberikan saran kepada Pengendali Data Pribadi atau Prosesor Data Pribadi agar mematuhi ketentuan dalam UU PDP
- Memantau dan memastikan kepatuhan terhadap UU PDP ini dan kebijakan Pengendali Data Pribadi atau Prosesor Data Pribadi
- Memberikan saran mengenai penilaian dampak Pelindungan Data Pribadi dan memantau kinerja Pengendali Data Pribadi dan Prosesor Data Pribadi
- Berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan Data Pribadi.

9

## Pengiriman dan Pengungkapan Data Pribadi

## Apakah Anda Melakukan Pengiriman Data Pribadi ke Luar Wilayah Indonesia?

Pengiriman atau transfer data pribadi dapat dilakukan antar Pengendali Data Pribadi dalam wilayah hukum Negara Republik Indonesia, atau transfer data pribadi kepada Pengendali Data Pribadi dan/atau Prosesor Data Pribadi di luar wilayah hukum Negara Republik Indonesia.

Praktik yang baik:

-  Pengendali Data Pribadi yang akan melakukan pengiriman Data Pribadi ke Luar Wilayah Indonesia memastikan bahwa Pengendali Data Pribadi telah mendapatkan persetujuan tertulis dari Subjek Data Pribadi atau memiliki dasar hukum lain untuk melakukan pemrosesan Data Pribadi (misalnya dalam hal pemenuhan pelindungan kepentingan yang sah (*vital interest*) Subjek Data Pribadi).
-  Dalam hal tidak terdapat persetujuan tertulis atau dasar hukum lain untuk melakukan pengiriman Data Pribadi, Pengendali Data Pribadi meminta persetujuan tambahan dari Subjek Data Pribadi sebelum melakukan pengiriman Data Pribadi (melalui formulir persetujuan tambahan atau persetujuan terhadap pembaharuan terhadap kebijakan privasi yang kemudian disampaikan kepada pemilik data secara langsung saat mereka menggunakan layanan atau melalui *email*).
-  Pengendali Data Pribadi memperhatikan ketentuan mengenai koordinasi dengan Kominfo (akan dirinci pada halaman pertanyaan selanjutnya).

## Apakah Anda Melakukan Pengiriman Data Pribadi ke Luar Wilayah Indonesia?

Contoh:

- Perusahaan multinasional yang sedari awal memahami bahwa untuk menjalankan operasionalnya memerlukan pengiriman Data Pribadi ke kantor pusatnya atau perusahaan lain dalam grup perusahaannya (di luar negeri), maka sedari awal proses pengumpulan Data Pribadi, perusahaan tersebut meminta persetujuan individual yang berkaitan termasuk juga untuk kegiatan pengiriman data ke luar wilayah Indonesia.
- Perusahaan jasa wisata dan travel di Australia menawarkan paket liburan di Australia kepada perusahaan di Indonesia. Dalam rangka program liburan karyawan, perusahaan Indonesia mengirimkan data ke perusahaan Australia tersebut untuk keperluan pemesanan hotel, tiket perjalanan, tiket wisata. Perusahaan Indonesia tersebut melakukan kegiatan transfer dan wajib memenuhi ketentuan transfer internasional berdasarkan regulasi PDP Indonesia.
- Perusahaan *e-commerce* di Indonesia mentransfer data pribadi pelanggannya ke perusahaan di Malaysia secara elektronik melalui server di Singapura – server transit. Sepanjang data tersebut dijamin tidak diakses atau diubah selama transit di Singapura, maka transfer hanya terjadi kepada perusahaan di Malaysia. Pengendali Data Pribadi wajib memenuhi ketentuan regulasi PDP di Indonesia.
- Penyedia layanan *cloud computing* menggunakan penyimpanan data di berbagai negara, penyedia tersebut tunduk pada ketentuan PDP, antara lain, menjamin dan menunjukkan kegiatan transfer data pribadi dilakukan dengan mengimplementasi upaya-upaya pelindungan data, seperti mengadopsi peraturan keanggotaan (*code of conduct*) asosiasi bisnis *cloud computing* yang relevan (contoh: Cloud Security Alliance dan Pan-Asian E-Commerce Alliance).

## 9.2

# Dalam Melakukan Pengiriman Data Pribadi ke Luar Wilayah Indonesia, Apakah Anda sudah Memenuhi Ketentuan Peraturan Perundang-Undangan tentang PDP?

Pengiriman Data Pribadi yang dikelola oleh Pengendali Data Pribadi yang berdomisili di wilayah negara Republik Indonesia ke luar wilayah Indonesia meliputi : (i) pengiriman Data Pribadi yang semula disimpan di Indonesia ke luar negeri; atau (ii) data WNI disimpan secara langsung pada *database* yang berada di luar negeri. Transfer data bukan berarti transit (*route*) yang mana data dikirim dari negara A ke B tetapi transit melalui C. Transit ke C ini bukan transfer data sepanjang pada saat transit, data pribadi tidak diakses atau diubah.

Dalam melakukan pengiriman data pribadi ke luar wilayah Indonesia, Pengendali Data Pribadi harus menerapkan ketentuan peraturan perundang-undangan mengenai pertukaran Data Pribadi lintas batas negara.

### Praktik yang baik:

 Pengendali Data Pribadi yang akan melakukan pengiriman Data Pribadi ke Luar Wilayah Indonesia memperhatikan dan memenuhi ketentuan mengenai pertukaran data pribadi lintas batas negara bukan hanya pada Peraturan Perundang-undangan di Indonesia tapi juga ketentuan pada negara tujuan transfer serta *code of conduct* yang ada pada sektor terkait.

### Contoh:

- Perusahaan asuransi Indonesia bekerja sama dengan perusahaan asuransi di Singapura dalam menyediakan layanan asuransi kepada masyarakat Indonesia. Perusahaan asuransi Indonesia harus memenuhi ketentuan transfer data pribadi pada Peraturan Perundang-undangan di Indonesia, termasuk melakukan koordinasi dengan Kominfo, serta memperhatikan ketentuan transfer data pada Singapura dan *code of conduct* pada sektor keuangan/asuransi.

## 9.2

# Dalam Melakukan Pengiriman Data Pribadi ke Luar Wilayah Indonesia, Apakah Anda sudah Memenuhi Ketentuan Peraturan Perundangan tentang PDP?

Praktik yang baik:

- Selain adanya persetujuan dari pemilik data, Pengendali Data Pribadi diperbolehkan melaporkan rencana dan proses pelaksanaan pengiriman Data Pribadi ke luar negeri ke Kominfo. Format laporan dapat diunduh pada tautan berikut: <https://komin.fo/FormLaporanTransferData>
- Bentuk laporan mengenai rencana pengiriman Data Pribadi harus memuat paling sedikit nama jelas negara tujuan, nama jelas subjek penerima, tanggal pelaksanaan, dan alasan/tujuan pengiriman.
- Untuk pelaksanaan, tidak terdapat format yang diatur dan dengan demikian Pengendali Data Pribadi disarankan melaporkan secara berkala mengenai pelaksanaan pengiriman Data Pribadi.
- Pengendali Data Pribadi dapat meminta advokasi berupa konsultasi dengan Kominfo (apabila diperlukan).
- Pengendali Data Pribadi harus pula mematuhi ketentuan mengenai pertukaran Data Pribadi lintas batas negara (saat ini belum terdapat peraturan yang dimaksud) tetapi PSE dapat mengadopsi peraturan anggota (*code of conduct*) asosiasi bisnis yang mengatur aspek *good practices* keamanan data dan PDP.

Contoh:

- Perusahaan multinasional yang memiliki kantor pusat di luar negeri umumnya akan mengirim/mempertukarkan banyak informasi elektronik (termasuk data pribadi) ke entitas lain di negara lain untuk kepentingan operasional. Dalam hal ini, ketentuan terkait dengan notifikasi pengiriman Data Pribadi kepada Kominfo menjadi relevan.
- Data diplomasi dapat memuat informasi tentang diri seseorang, kementerian luar negeri dalam melakukan penyebarluasan data diplomasi, yaitu kegiatan pemberian akses, pendistribusian, dan pertukaran data perlu mematuhi ketentuan PDP, khususnya dalam hal terdapat data pribadi yang dikumpulkan dan diolah melalui sistem elektronik sebagai bagian dari data diplomasi. Hal ini sebagaimana ditegaskan dalam peraturan menteri luar negeri mengenai tata kelola data diplomasi kementerian luar negeri dan perwakilan republik Indonesia.

## 9.2

# Dalam Melakukan Pengiriman Data Pribadi ke Luar Wilayah Indonesia, Apakah Anda sudah Memenuhi Ketentuan Peraturan Perundangan tentang PDP?

### **Informasi UU PDP:**

Dalam melakukan transfer data pribadi ke luar wilayah hukum Negara Republik Indonesia, Pengendali Data Pribadi wajib:

1. Memastikan negara tempat kedudukan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi yang menerima transfer Data Pribadi memiliki tingkat Pelindungan Data Pribadi yang setara atau lebih tinggi dari pengaturan dalam UU PDP.
2. Dalam hal nomor 1 tidak terpenuhi, maka Pengendali Data Pribadi wajib memastikan terdapat Pelindungan Data Pribadi yang memadai dan bersifat mengikat.
3. Dalam hal nomor 1 dan 2 tidak dapat terpenuhi, maka Pengendali Data Pribadi wajib mendapatkan persetujuan Subjek Data Pribadi.

## 9.3

# Apakah Anda Memiliki Kebijakan dan Prosedur dalam hal Terdapat Permintaan dari Aparat Penegak Hukum Terkait Data Pribadi yang Anda Kelola?

Pengendali Data Pribadi wajib memberikan akses ke data pribadi yang terdapat dalam sistem elektronik yang dikuasai/diselenggarakan oleh Pengendali Data Pribadi tersebut atas permintaan yang sah dari aparat penegak hukum (kepolisian, jaksa, dan Penyidik PNS) dan K/L di Indonesia. Data pribadi yang diminta adalah yang relevan dan sesuai dengan kebutuhan penegakan hukum pidana dan pengawasan K/L yang permintaan aksesnya dikeluarkan secara resmi sesuai ketentuan peraturan perundang-undangan.

Praktik yang baik:

- Pengendali Data Pribadi menyertakan dalam kebijakan privasi atau formulir persetujuan pada saat pengumpulan data adanya ketentuan pemberian akses terhadap data pribadi yang diajukan oleh APH dan/atau K/L dalam rangka pengawasan K/L dan penegakan hukum pidana.
- Pengendali Data Pribadi menyusun dan menyampaikan aturan internal kepada semua karyawan dan afiliasinya terkait kebijakan dan mekanisme perusahaan dalam memberikan akses ke data pribadi yang dikuasai/diselenggarakannya dalam rangka pengawasan K/L dan penegakan hukum pidana.
- Pengendali Data Pribadi menerapkan ketentuan peraturan yang mengatur mengenai permintaan akses terhadap informasi dan/atau dokumen elektronik yang berlaku di Kominfo dan/atau instansi penyelenggara negara lain.

## 9.3

# Apakah Anda Memiliki Kebijakan dan Prosedur dalam hal Terdapat Permintaan dari Aparat Penegak Hukum Terkait Data Pribadi yang Anda Kelola?

Contoh:

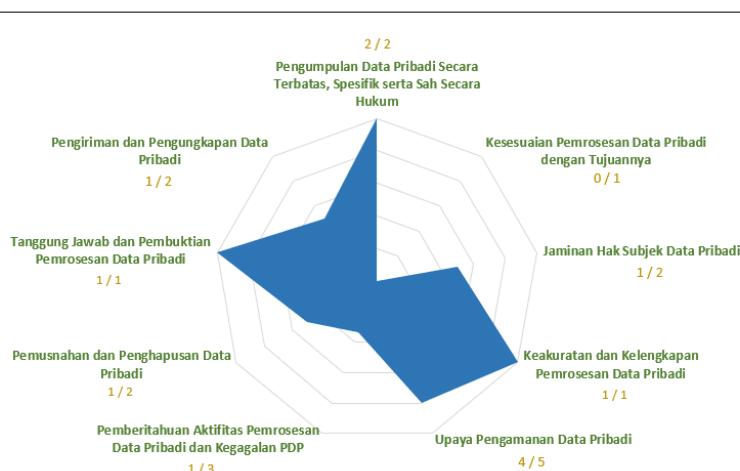
- Perusahaan telekomunikasi wajib memberikan informasi pelanggan dalam hal informasi dibutuhkan untuk proses peradilan pidana. Perusahaan telekomunikasi menginformasikan hal ini kepada pelanggan dalam syarat dan ketentuan pada saat pengaktivasian produk.
- Ditjen Imigrasi Kementerian Hukum dan HAM menyelenggarakan Sistem Informasi Manajemen Keimigrasian ("**SIMKIM**") yaitu sistem informasi dan komunikasi yang digunakan untuk mengumpulkan, mengolah, dan menyajikan informasi guna mendukung operasional, manajemen, dan pengambilan keputusan dalam melaksanakan fungsi keimigrasian (perihal lalu lintas orang). Berdasarkan UU Keimigrasian, SIMKIM dapat diakses oleh instansi dan/atau lembaga pemerintahan terkait sesuai dengan tugas dan fungsinya. Pemberian akses ini wajib memperhatikan ketentuan PDP, antara lain, pengamanan dan kerahasiaan data pribadi, serta adanya DPO.

# **HASIL ASESMEN IMPLEMENTASI PELINDUNGAN DATA PRIBADI**

# Hasil Asesmen

## HASIL ASESMEN IMPLEMENTASI PELINDUNGAN DATA PRIBADI

Percentase Kepatuhan PDP	10 / 16	63%	Menengah
--------------------------	---------	-----	----------



### Keterangan Persentase Kepatuhan PDP



91% - 100 % : Tinggi



51% - 90% : Menengah



0% - 50% : Rendah

# Hasil Asesmen

## 1. Pengumpulan Data Pribadi Secara Terbatas, Spesifik serta Sah Secara Hukum Nilai : 2 / 2 Sudah Memenuhi

Anda sudah memenuhi semua poin asesmen dalam kategori ini.

## 2. Kesesuaian Pemrosesan Data Pribadi dengan Tujuannya Nilai : 0 / 1 Tidak Memenuhi

Saran

Anda harus memastikan bahwa Data Pribadi yang Anda proses:

1. memadai - cukup untuk memenuhi tujuan yang Anda nyatakan;
2. relevan - Anda hanya dapat mengumpulkan data yang berkaitan langsung dengan pemrosesan Anda; dan
- 2.1 3. terbatas pada apa yang perlu - Anda tidak mengumpulkan Data Pribadi lebih dari yang Anda butuhkan untuk pencapaian tujuan.

Saran lebih lanjut terkait poin ini dapat diakses pada file Panduan halaman 34-35 (Apakah Pemrosesan Data Pribadi yang Anda Lakukan telah sesuai dengan Tujuan Pemrosesannya?).

## 3. Jaminan Hak Subjek Data Pribadi Nilai : 1 / 2 Kurang

Saran

- Anda harus memiliki prosedur untuk memastikan untuk menanggapi permintaan salinan Data Pribadi dari subjek Data Pribadi
- Anda harus memiliki mekanisme yang memungkinkan subjek Data Pribadi memiliki akses untuk mendapatkan informasi yang diinginkan terkait pemrosesan Data Pribadinya.
- 3.2 • Dalam memenuhi permintaan perolehan Data Pribadi dari Subjek Data Pribadi, Anda harus memastikan informasi tersebut disampaikan dengan menggunakan metode yang aman.
  - Data Pribadi yang diperoleh oleh Subjek Data Pribadi harus dalam format terstruktur dan umum digunakan.
  - Anda harus memastikan bahwa data yang diminta adalah Data Pribadi dari Subjek Data Pribadi yang melakukan permintaan akses atau salinan Data Pribadi.
  - Saran lebih lanjut dapat diakses pada file Panduan halaman 42 (Apakah Anda Menyediakan Akses atau Kesempatan bagi Subjek Data Pribadi Untuk Memperoleh Salinan Data Pribadi yang Pernah Diserahkan?).

## 4. Keakuratan dan Kelengkapan Pemrosesan Data Pribadi Nilai : 1 / 1 Sudah Memenuhi

Anda sudah memenuhi semua poin asesmen dalam kategori ini.

## 5. Upaya Pengamanan Data Pribadi Nilai : 4 / 5 Kurang

Saran

- 5.5 • Anda harus memiliki kebijakan pengelolaan Data Pribadi atau aturan internal atau sejenisnya (internal-facing privacy policy) dan mengambil langkah-langkah untuk memastikan kebijakan tersebut diterapkan.
- Apabila memungkinkan dan dibutuhkan, Anda dapat memiliki kebijakan tambahan dan memastikan bahwa kontrol diterapkan.
  - Anda harus meninjau kebijakan dan tindakan secara berkala dan jika perlu, memperbaikinya.
  - Saran lebih lanjut terkait poin ini dapat diakses pada file Panduan halaman 54-55 dan 62 (Apakah Anda Memiliki Aturan Internal Terkait Hal Pemrosesan Data Pribadi?).
- 5.6 • Anda harus memiliki program sosialisasi, termasuk pelatihan (training), terhadap aturan internal sebagai salah satu langkah awal untuk memastikan kebijakan diketahui dan kemudian diterapkan oleh seluruh pegawai dan pihak terkait.
- Saran lebih lanjut terkait poin ini dapat diakses pada file Panduan halaman 56 dan 62 (Apakah Anda Melakukan Sosialisasi kepada Seluruh Pegawai mengenai Aturan Internal Terkait Pemrosesan Data Pribadi?).

## Keterangan

100 % : Sudah Memenuhi

1-49% : Sangat Kurang

50-99% : Kurang

0% : Tidak memenuhi

# Hasil Asesmen

## 6. Pemberitahuan Aktifitas Pemrosesan Data Pribadi dan Kegagalan PDP

Nilai : 1 / 3

Sangat Kurang

### Saran

- 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.
- Jika terjadi kegagalan pelindungan Data Pribadi, Anda wajib menyampaikan pemberitahuan secara tertulis paling lambat 3x24 jam kepada Subjek data Pribadi.

- 6.2 • Dalam rangka melaksanakan prinsip pelindungan Data Pribadi dalam melakukan pemrosesan Data Pribadi, Anda harus menginformasikan kepada subjek Data Pribadi tentang bagaimana akan memproses Data Pribadi mereka.
- Anda harus memastikan bahwa Anda memberi tahu individu tentang pemrosesan Anda dengan cara yang mudah diakses dan dipahami. Anda harus menggunakan bahasa yang jelas dan sederhana.
  - Saran lebih lanjut terkait poin ini dapat diakses pada file Panduan halaman 66-68 (Apakah Anda Memiliki Mekanisme Pemberitahuan secara Tertulis Kepada Subjek Data Pribadi jika Terjadi Kegagalan dalam Pelindungan Data Pribadi?).

- Anda harus menyediakan saluran atau kanal aduan yang dapat digunakan oleh subjek Data Pribadi untuk melaporkan dampak terhadap kegagalan pelindungan Data Pribadi.

- 6.3 • Saran lebih lanjut terkait poin ini dapat diakses pada file Panduan halaman 69-70 (Apakah Anda Menyediakan Kanal Aduan yang Dapat Digunakan oleh Subjek Data Pribadi untuk Melaporkan Dampak terhadap Kegagalan Pelindungan Data Pribadi?).

## 7. Pemusnahan dan Penghapusan Data Pribadi

Nilai : 1 / 2

Kurang

### Saran

- Anda harus memiliki mekanisme untuk memastikan penghapusan dan pemusnahan Data Pribadi dari Sistem Elektronik Anda sebagaimana ketentuan Pasal 43 dan 44 UU PDP.

- Pengendali data harus melaksanakan permintaan penghapusan ini kecuali ada suatu dasar hukum yang jelas mengapa data tersebut harus tetap disimpan contohnya demi kepentingan proses penegakan hukum.

- 7.1 • Jika permintaan penghapusan dilayangkan terkait dengan tujuan pemrosesan yang telah tercapai, maka Anda harus melakukan pemeriksaan lebih lanjut jika ada data lain yang masih Anda simpan namun tidak ada tujuan yang relevan.
- Anda wajib memberitahukan penghapusan dan/atau pemusnahan Data Pribadi kepada Subjek Data Pribadi
  - Saran lebih lanjut dapat diakses pada file Panduan halaman 74-76 (Apakah Anda Menyediakan Mekanisme Penghapusan dan/atau Pemusnahan Data Pribadi sesuai dengan Ketentuan Peraturan Perundang-Undangan?)

## 8. Tanggung Jawab dan Pembuktian Pemrosesan Data Pribadi

Nilai : 1 / 1

Sudah Memenuhi

Anda sudah memenuhi semua poin asesmen dalam kategori ini.

## 9. Pengiriman dan Pengungkapan Data Pribadi

Nilai : 1 / 2

Kurang

### Saran

- Anda perlu memastikan bahwa tingkat pelindungan Data Pribadi di negara tujuan sudah setara dengan ketentuan UU PDP atau sudah memadai.

- 9.2 • Jika Anda melakukan pengiriman Data Pribadi ke luar wilayah Indonesia berdasarkan pada persetujuan, maka Anda perlu juga memiliki kontrak dengan importir data yang memuat ketentuan pelindungan data berdasarkan UU PDP. Atas dasar itu, persetujuan saja bukan menjadi alasan utama yang bisa mengesampingkan kewajiban Anda dalam UU PDP.

- Saran lebih lanjut dapat diakses pada file Panduan halaman 83-84 (Dalam Melakukan Pengiriman Data Pribadi ke Luar Wilayah Indonesia, Apakah Anda sudah Memenuhi Ketentuan Peraturan Perundang-Undangan tentang PDP?).

## Keterangan

100 % : Sudah Memenuhi

1-49% : Sangat Kurang

50-99% : Kurang

0% : Tidak memenuhi

# KONTAK

## Tim Pengawasan Pelindungan Data Pribadi

Direktorat Pengendalian Aplikasi Informatika

Direktorat Jenderal Aplikasi Informatika

Kementerian Komunikasi dan Informatika

### Koordinasi Insiden



[pengendalianaptika@kominfo.go.id](mailto:pengendalianaptika@kominfo.go.id)



0812 2216 5580

### Aduan dan Konsultasi PDP



[aduanpdp@kominfo.go.id](mailto:aduanpdp@kominfo.go.id)



0811 1951 4444



KOMINFO

# Pelindungan Data Pribadi

**Aman, Andal dan Bertanggung Jawab**

Direktorat Pengendalian Aplikasi Informatika  
Direktorat Jenderal Aplikasi Informatika  
Kementerian Komunikasi dan Informatika