



# Sosialisasi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Prof. Dr Sinta Dewi Rosadi, SH, LL.M

Departemen Hukum Teknologi Informasi dan Kekayaan Intelektual,  
FH, UNPAD

## SUBSTANSI REGULASI

Definisi & Ruang Lingkup	Sanksi Administratif
Asas Undang-Undang	Kelembagaan
Jenis Data Pribadi	Kerjasama Internasional
Hak Subjek Data Pribadi	Partisipasi Masyarakat
Pemrosesan Data Pribadi	Penyelesaian Sengketa dan Hukum Acara
Prinsip dan pemrosesan Data Pribadi	Larangan dalam Penggunaan Data Pribadi
<i>Joint controller</i>	Ketentuan Pidana
Kewajiban Pengendali dan Prosesor Data Pribadi	Ketentuan Perlaiihan dan Penutup
Transfer Data Pribadi	

# GAMBARAN UMUM UU PDP

Kehadiran UU PDP akan memberikan sebuah regulasi primer yang universal bagi Indonesia, untuk menjagadan mengatur perlindungan data pribadi masyarakat Indonesia, di mana pun data mereka berada.

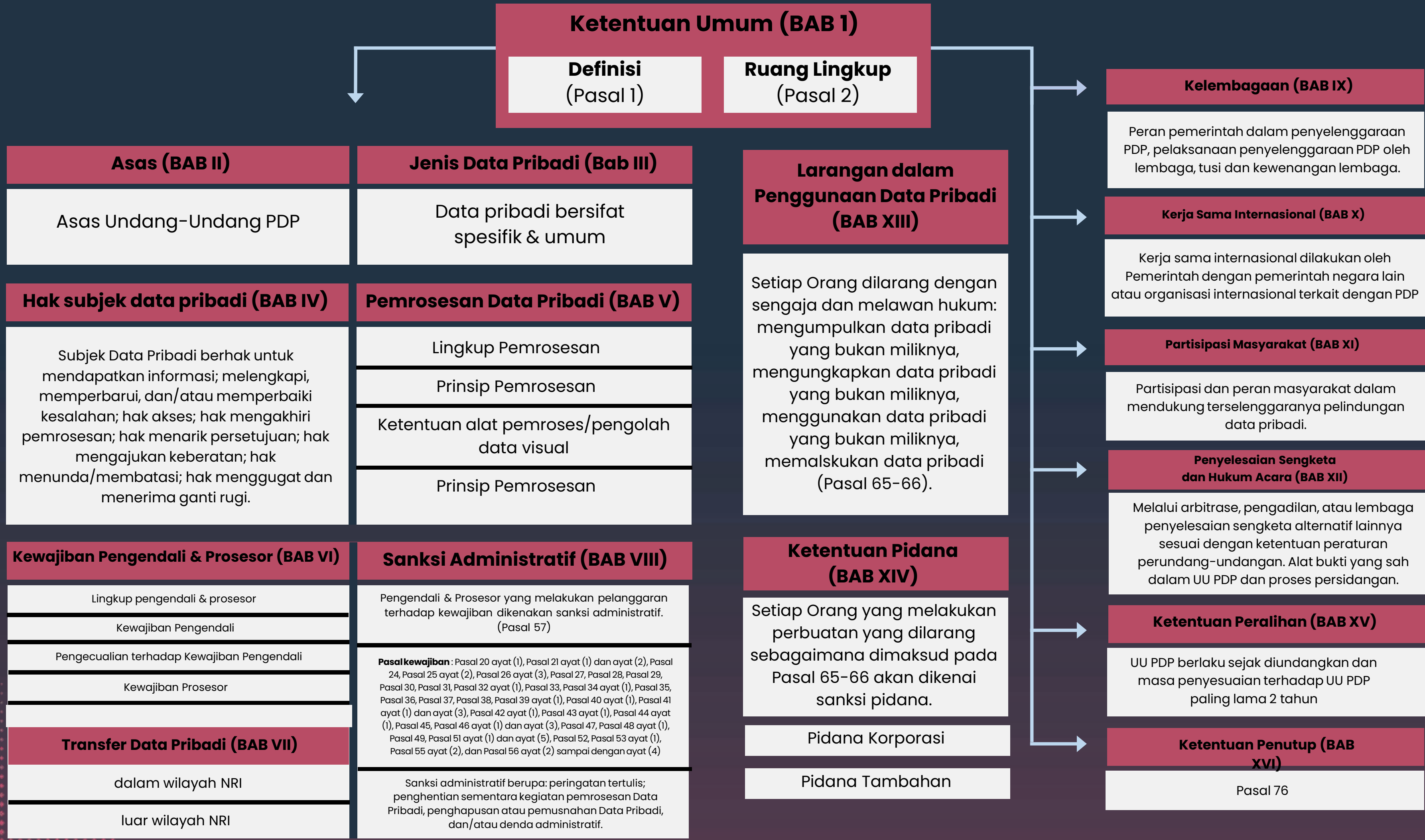
STATUS: Telah disahkan oleh DPR dan Pemerintah dan telah diundangkan (UU No. 27/2022)

**Pertukaran Data dalam Wilayah NKRI**

**Pertukaran Data antara NKRI dengan wilayah negara lain**

**Pemerintah/Sektor Publik**

**Sektor Privat**



# Ketentuan Umum (BAB I)

**Definisi**  
(Pasal 1)

**Ruang Lingkup**  
(Pasal 2)

## Asas (BAB II)

Asas Undang-Undang PDP

## Jenis Data Pribadi (Bab III)

Data pribadi bersifat spesifik & umum

## Larangan dalam Penggunaan Data Pribadi (BAB XIII)

Setiap Orang dilarang dengan sengaja dan melawan hukum: mengumpulkan data pribadi yang bukan miliknya, mengungkapkan data pribadi yang bukan miliknya, menggunakan data pribadi yang bukan miliknya, memalsukan data pribadi (Pasal 65-66).

## Kelembagaan (BAB IX)

Peran pemerintah dalam penyelenggaraan PDP, pelaksanaan penyelenggaraan PDP oleh lembaga, tuisi dan kewenangan lembaga.

## Hak subjek data pribadi (BAB IV)

Subjek Data Pribadi berhak untuk mendapatkan informasi; melengkapi, memperbarui, dan/atau memperbaiki kesalahan; hak akses; hak mengakhiri pemrosesan; hak menarik persetujuan; hak mengajukan keberatan; hak menunda/membatasi; hak menggugat dan menerima ganti rugi.

## Pemrosesan Data Pribadi (BAB V)

- Lingkup Pemrosesan
- Prinsip Pemrosesan
- Ketentuan alat pemroses/pengolah data visual
- Prinsip Pemrosesan

## Kerja Sama Internasional (BAB X)

Kerja sama internasional dilakukan oleh Pemerintah dengan pemerintah negara lain atau organisasi internasional terkait dengan PDP

## Kewajiban Pengendali & Proesor (BAB VI)

- Lingkup pengendali & proesor
- Kewajiban Pengendali
- Pengecualian terhadap Kewajiban Pengendali
- Kewajiban Proesor

## Sanksi Administratif (BAB VIII)

Pengendali & Proesor yang melakukan pelanggaran terhadap kewajiban dikenakan sanksi administratif. (Pasal 57)

**Pasal kewajiban :** Pasal 20 ayat (1), Pasal 21 ayat (1) dan ayat (2), Pasal 24, Pasal 25 ayat (2), Pasal 26 ayat (3), Pasal 27, Pasal 28, Pasal 29, Pasal 30, Pasal 31, Pasal 32 ayat (1), Pasal 33, Pasal 34 ayat (1), Pasal 35, Pasal 36, Pasal 37, Pasal 38, Pasal 39 ayat (1), Pasal 40 ayat (1), Pasal 41 ayat (1) dan ayat (3), Pasal 42 ayat (1), Pasal 43 ayat (1), Pasal 44 ayat (1), Pasal 45, Pasal 46 ayat (1) dan ayat (3), Pasal 47, Pasal 48 ayat (1), Pasal 49, Pasal 51 ayat (1) dan ayat (5), Pasal 52, Pasal 53 ayat (1), Pasal 55 ayat (2), dan Pasal 56 ayat (2) sampai dengan ayat (4)

Sanksi administratif berupa: peringatan tertulis; penghentian sementara kegiatan pemrosesan Data Pribadi, penghapusan atau pemusnahan Data Pribadi, dan/atau denda administratif.

## Ketentuan Pidana (BAB XIV)

Setiap Orang yang melakukan perbuatan yang dilarang sebagaimana dimaksud pada Pasal 65-66 akan dikenai sanksi pidana.

- Pidana Korporasi
- Pidana Tambahan

## Partisipasi Masyarakat (BAB XI)

Partisipasi dan peran masyarakat dalam mendukung terselenggaranya perlindungan data pribadi.

## Transfer Data Pribadi (BAB VII)

- dalam wilayah NRI
- luar wilayah NRI

## Penyelesaian Sengketa dan Hukum Acara (BAB XII)

Melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan. Alat bukti yang sah dalam UU PDP dan proses persidangan.

## Ketentuan Peralihan (BAB XV)

UU PDP berlaku sejak diundangkan dan masa penyesuaian terhadap UU PDP paling lama 2 tahun

## Ketentuan Penutup (BAB XVI)

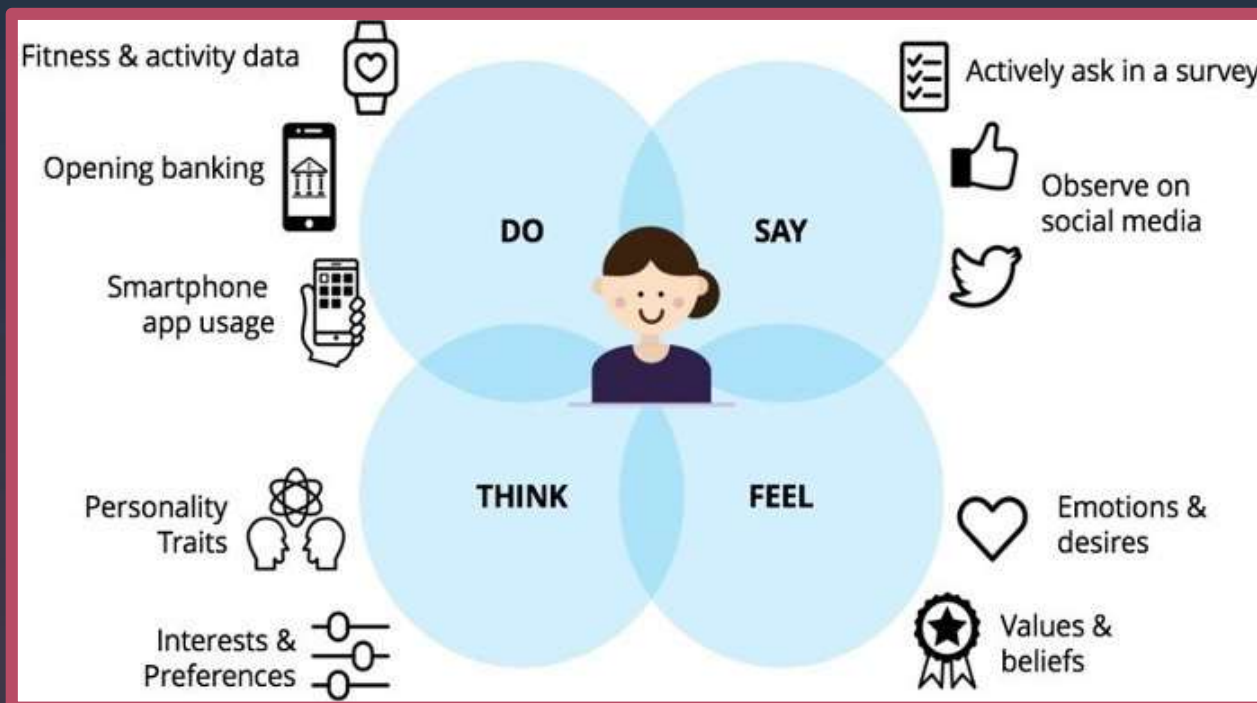
Pasal 76

# Apa itu Data Pribadi?

Definisi Data Pribadi  
dari UU PDP

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 non elektronik.

Cakupan Data Pribadi sangat luas yang meliputi aktivitas (*do, say, think, and feel*) manusia di dunia digital, yang diperoleh dari **berbagai sumber** dan dapat diproses secara **masif dan otomatis** menggunakan berbagai teknologi.



Dari berbagai data pribadi tersebut, terdapat data pribadi spesifik yang bersifat spesifik yang memerlukan perlindungan ekstra.

## Jenis Data Pribadi: Data Pribadi bersifat Spesifik

- o Data dan Informasi Kesehatan
- o Data Biometrik
- o Data Genetika
- o Catatan Kejahatan
- o Data Anak
- o Data Keuangan Pribadi
- o **Data lainnya sesuai dengan ketentuan peraturan perundang-undangan**

## Jenis Data Pribadi: Data Pribadi bersifat Umum

- o Nama lengkap
- o Jenis kelamin
- o Kewarganegaraan
- o Agama
- o Status perkawinan
- o **Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang**

Data Pribadi yang diproses oleh organisasi pengendali data pribadi dapat meliputi **Data Pribadi pegawai/karyawan dan/atau Data Pribadi pengguna layanan/aplikasi.**

# MENGENAL PARA PIHAK DALAM PEMROSESAN DATA PRIBADI

## 1 Pengendali Data Pribadi

Setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.

Pemrosesan Data Pribadi dapat dilakukan oleh 2 (dua) atau lebih Pengendali Data Pribadi, namun harus memenuhi syarat minimal antara lain terdapat perjanjian, terdapat tujuan yang saling berkaitan, dan terdapat narahubung yang ditunjuk secara bersama-sama.

## 2 Prosesor Data Pribadi

Setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan Data Pribadi atas nama Pengendali Data Pribadi.

## 3 Subjek Data Pribadi

Orang perseorangan yang pada dirinya melekat Data Pribadi.

## 4 Lembaga Pelindungan Data Pribadi

LPDP sebagai Pengawas UU PDP yang akan ditentukan oleh Presiden.

# Lingkup Pemrosesan Data Pribadi



Pemerolehan & pengumpulan



Pengolahan dan penganalisisan



Penyimpanan



Perbaikan dan pembaruan



Penampilan, Pengumuman, Transfer, Penyebarluasan, atau Pengungkapan



Penghapusan atau pemusnahan

# PEMROSESAN DATA PRIBADI

## Prinsip Pemrosesan Data Pribadi

- Pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan;
- Pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya;
- Pemrosesan Data Pribadi dilakukan dengan menjamin hak Subjek Data Pribadi;
- Pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan;
- Pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, perubahan yang tidak sah, penyalahgunaan, kerusakan, dan/atau penghilangan Data Pribadi;
- Pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan dan aktivitas, serta kegagalan Pelindungan Data Pribadi;
- Data Pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan Subjek Data Pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan;
- Pemrosesan Data Pribadi dilakukan secara bertanggungjawab dan dapat dibuktikan secara jelas

## Dasar Pemrosesan Data Pribadi

- Persetujuan yang sah secara eksplisit dari Subjek Data Pribadi;
- Pemenuhan kewajiban perjanjian;
- Pemenuhan kewajiban hukum dari Pengendali Data Pribadi;
- Pemenuhan perlindungan kepentingan vital Subjek Data Pribadi;
- Pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengandali Data Pribadi;
- Pemenuhan kepentingan yang sah lainnya (dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan)

# HAK SUBJEK DATA PRIBADI



Subjek Data Pribadi adalah orang perseorangan yang pada dirinya melekat Data Pribadi.



meminta informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, akuntabilitas pihak yang meminta Data Pribadi



mengakhiri, pemrosesan, menghapus, memusnahkan Data Pribadi miliknya



menunda/membatasi pemrosesan



melengkapi, memperbarui, dan/atau memperbaiki kesalahan/ketidakakuratan



menarik kembali persetujuan pemrosesan



menggugat dan menerima ganti rugi atas pelanggaran



mendapatkan akses dan memperoleh salinan



mengajukan keberatan atas tindakan pengambilan keputusan yang hanya berdasar pemrosesan otomatis



mendapatkan, menggunakan, mengirimkan Data Pribadinya



menggunakan dan mengirimkan Data Pribadi miliknya

*Hak-hak Subjek Data Pribadi sebagaimana dimaksud tidak mutlak dan dapat dikecualikan untuk dasar dan kepentingan tertentu.*

# KEWAJIBAN PENGENDALI DATA PRIBADI

## Prinsip PDP

Pengumpulan secara terbatas, spesifik, sah, dan transparan

Sesuai dengan tujuan

Menjamin hak Subjek Data

Akurat lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggung-jawabkan

Melindungi kemanan

Pemberitahuan tujuan, aktivitas pemrosesan dan kegagalan perlindungan

Penghapusan dan pemusnahan berdasar masa retensi atau permintaan

Bertanggung jawab dan dapat dibuktikan secara jelas



## Kewajiban yang Bersumber pada Hak

menyampaikan informasi

memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan (dalam waktu 3x24 jam)

memberikan akses (dalam waktu 3x24 jam) serta menolak memberikan akses

mengakhiri pemrosesan, menghapus, dan memusnahkan

menghentikan pemrosesan (dalam waktu 3x24 jam)

penundaan dan pembatasan (dalam waktu 3x24 jam)

## Kewajiban sebagai Wujud Kepatuhan/Compliance

persetujuan pemrosesan data anak & disabilitas

melaksanakan perintah lembaga

melakukan perekaman, melakukan analisis dampak PDP

melakukan perekaman, melakukan analisis dampak PDP

akurasi, kelengkapan dan konsistensi data pribadi

menunjuk pejabat/petugas PDP

menjaga keamanan dan kerahasiaan data pribadi

pengawasan

melakukan perekaman, melakukan analisis dampak PDP

pertanggungjawaban pemenuhan kewajiban

memenuhi ketentuan transfer Data Pribadi

pemrosesan secara terbatas dan spesifik, sah secara hukum, dan transparan

pemberitahuan kegagalan perlindungan dan pengalihan data pribadi (dalam waktu 3x24 jam)

pemberitahuan penghapusan dan pemusnahan data pribadi

memperbarui, memperbaiki kesalahan serta ketidakakuratan data pribadi

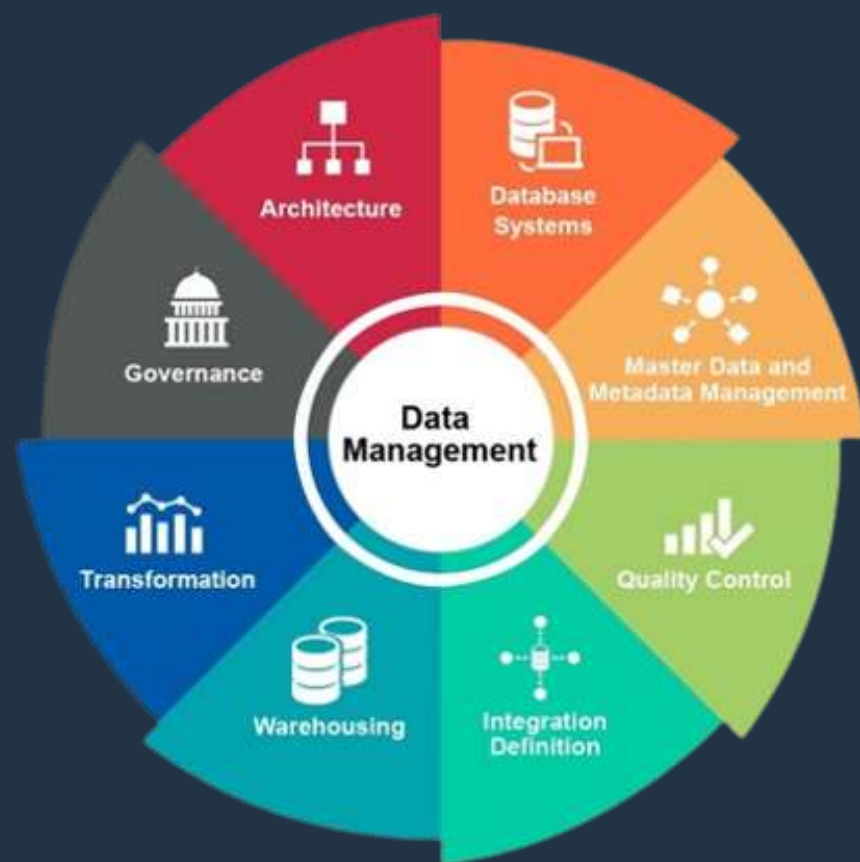
*Kewajiban Pengendali Data Pribadi sebagaimana dimaksud tidak mutlak dan dapat dikecualikan untuk dasar dan kepentingan tertentu.*

# KEWAJIBAN PENGENDALI DATA PRIBADI – MENUNJUK DPO

Dalam hal tertentu, Pengendali Data Pribadi wajib menunjuk pejabat/petugas yang melaksanakan fungsi perlindungan data pribadi (PPDP/DPO/Data Protection Officer)

Setidaknya dibutuhkan 140.917 orang PPDP untuk memenuhi kebutuhan PPDP di Indonesia

(Kajian Grand Design Pembentukan Ekosistem PPDP, Kemkominfo, 2021)



PPDP/DPO membantu departemen/unit pengelola data dalam penerapan langkah teknis dan organisasi agar patuh dengan aturan perlindungan data pribadi dalam seluruh siklus pemrosesan.

## TUGAS PDP

- menginformasikan dan memberikan saran kepada Pengendali Data Pribadi atau Proesor Data Pribadi agar mematuhi ketentuan dalam Undang- Undang ini;
- memantau dan memastikan kepatuhan terhadap Undang-Undang ini dan kebijakan PengendaliData Pribadi atau Proesor Data Pribadi;
- memberikan saran mengenai penilaian dampak Pelindungan Data Pribadi dan memantau kinerja Pengendali Data Pribadi dan Proesor Data Pribadi; dan
- berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan Data Pribadi.

# KEWAJIBAN PENGENDALI DATA PRIBADI - Transfer ke Luar Indonesia



Secara default seluruh Pengendali Data Pribadi data pribadi wajib memenuhi seluruh ketentuan PDP antara lain:

## Prinsip PDP – Dasar Pemrosesan (Legal Basis) – Hak Subjek Data – Kewajiban Pengendali Data Pribadi

Pengendali Data Pribadi dapat melakukan transfer Data Pribadi kepada Pengendali Data Pribadi dan/atau Prosesor Data Pribadi di luar wilayah hukum Negara Republik Indonesia sesuai dengan ketentuan yang diatur dalam Undang-Undang PDP.

*Ketentuan yang secara berjenjang wajib dipenuhi untuk transfer ke luar wilayah Indonesia*



1  
Kesetaraan  
(Adequacy)

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.

2  
Pelindungan Data  
Pribadi yang  
Mengikat

Memastikan terdapat Pelindungan Data Pribadi yang memadai dan bersifat mengikat.

3  
Persetujuan

Mendapatkan persetujuan Subjek Data Pribadi.

# KEKECUALIAN/EXEMPTION

- Hak atas data pribadi tidak berlaku secara absolut banyak negara menerapkan kekecualian.
- Secara umum, kekecualian diterapkan apabila kepentingan nasional atau kepentingan public lebih besar daripada kepentingan seseorang.
- Prinsip berimbang/Balance Principles dan Penerapan harus hati-hati jangan sampai merugikan hak data pribadi
- Diatur dalam ketentuan undang-undang.

1

## MENERAPKAN KEKECUALIAN

Apabila akan menerapkan kekecualian maka subjek data harus mendapatkan informasi :

- Akan diterapkan kekecualian;
- Alasan pengecualian;
- Subjek data berhak mengajukan keberatan pada lembaga pengawas;

2

## KEWAJIBAN YANG DIKECUALIKAN

- Hak subjek data
- Kewajiban notifikasi terjadinya kegagalan dalam perlindungan/data breach
- Prinsip transparansi
- Prinsip pembatasan tujuan

# PENGECUALIAN HAK SUBJEK DATA DAN KEWAJIBAN PENGENDALI DATA

## Beberapa hak dapat dikecualikan untuk kepentingan (Pasal 15):

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

## Beberapa kewajiban Pengendali Data dapat dikecualikan (Pasal 50):

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

## Ayat 2

- Pengecualian dilaksanakan hanya dalam rangka pelaksanaan Undang-Undang
- Harus dibuat aturan pelaksana yang jelas
- Di Inggris atau EU selalu mengacu pada Charter HAM
- Hanya boleh dilakukan oleh Pihak yang berwenang seperti Penegak Hukum atau yang memiliki kewenangan untuk Penegakan Hukum
- Berdasarkan Undang-Undang
- Contoh : Polisi, Hakim, Jaksa, KPK, Penyidik Pegawai Negeri Sipil, BNN

# KETENTUAN SANKSI DALAM RUU PELINDUNGAN DATA PRIBADI

## SANKSI PIDANA

mengungkapkan Data Pribadi yang bukan miliknya



pidana penjara maks 4 tahun  
pidana denda maks 4 miliar

memperoleh atau mengumpulkan Data Pribadi



pidana penjara maks 5 tahun  
pidana denda maks 5 miliar

menggunakan Data Pribadi yang dimilikinya



membuat Data Pribadi palsu atau memalsukan Data Pribadi

pidana penjara maks 6 tahun  
pidana denda maks 6 miliar

## SANKSI ADMINISTRATIF

Pelanggaran pemenuhan ketentuan mengenai kewajiban

- peringatan tertulis
- penghentian sementara kegiatan pemrosesan Data Pribadi
- penghapusan atau pemusnahan Data Pribadi
- denda administratif

denda administratif maksimal 2% pendapatan/penerimaan tahunan terhadap variabel pelanggaran

## PERDATA

**Subjek Data Pribadi berhak menggugat dan menerima ganti rugi** atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.

### EFEKTIF

memberikan perlindungan atas data pribadi sebagai hak konstitusional

### PROPORSIONAL

mencapai keseimbangan dari kepentingan para pihak

### EFEK JERA

tidak diulangi oleh pelaku dan tidak dilakukan oleh pihak lain

# KETENTUAN PERALIHAN DAN KETENTUAN PENUTUP

## Pasal 74

Pada saat Undang-Undang ini mulai berlaku, Pengendali Data Pribadi, Prosesor Data Pribadi, dan pihak lain yang terkait dengan Pemrosesan Data Pribadi, wajib menyesuaikan dengan ketentuan pemrosesan Data Pribadi berdasarkan Undang-Undang ini paling lama 2 (dua) tahun sejak Undang-Undang ini diundangkan.

## Pasal 75

Pada saat Undang-Undang ini mulai berlaku, semua ketentuan peraturan perundang-undangan yang mengatur mengenai Pelindungan Data Pribadi, dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam Undang-Undang.

## Pasal 76

Undang-Undang ini mulai berlaku pada tanggal diundangkan.

# STRATEGI BAGI ORGANISASI

**KULTUR**

**SUMBER DAYA  
MANUSIA**

**TEKNOLOGI**

**MITIGASI RISIKO**  
(Jaringan, Sistem, Data)

**PERSIAPAN**

- Mengidentifikasi jenis data pribadi, tujuan, dan legal basis (persetujuan, kontrak, kewenangan, dsb) dari data pribadi yang dikumpulkan, diproses, diberikan ke pihak lain, disimpan, dan dimusnahkan.
- Mengevaluasi semua perjanjian/kontrak dengan pihak ketiga (prosesor, penyedia komputasi awan, jaringan pengiklanan, dsb) yang melibatkan data pribadi.
- Membuat dan/atau mengevaluasi Kebijakan privasi/PDP (privacy/data protection policy) yang komprehensif, ditampilkan secara jelas, & dapat dipahami oleh pengguna.
- Menyusun kebijakan/SOP internal yang mengatur pemrosesan data pribadi (mulai dari pengumpulan hingga penghapusan/pemusnahan).
- Menunjuk pejabat/petugas untuk menangani PDP (Data Protection Officer) di internal organisasi.

**PELAKSANAAN**

- Memastikan dan melaksanakan kepatuhan terhadap regulasi PDP dan kebijakan/SOP internal
- Menerapkan sistem keamanan yang andal dalam pemrosesan maupun penyimpanan data pribadi
- Menggunakan alat/teknologi yang menunjang privasi dan perlindungan data pribadi pengguna (privacy-enhancing tools)
- Menyediakan layanan/kontak bantuan untuk pengguna
- Memberikan edukasi/pelatihan mengenai kebijakan dan implementasi PDP untuk semua pegawai
- Mendukung kerja-kerja pejabat/pertugas yang melaksanakan PDP (Data Protection Officer)

**PENGAWASAN & MITIGASI**

- Melakukan evaluasi secara berkala terhadap aktivitas pemrosesan data pribadi
- Penerapan risk assesment dan prosedur mitigasi jika terjadi kebocoran data pribadi
- Mendokumentasikan rekam jejak pemrosesan, permintaan informasi dari subjek data pribadi ataupun otoritas berwenang
- Berkoordinasi dan melapor kepada Pemerintah/lembaga berwenang jika terjadi kebocoran data pribadi.

# ATURAN DAN KEPATUHAN HUKUM

## EFFEKTIFITAS REGULASI

1

### Revolusi dalam Penegakan

Denda hingga 2% dari pendapatan atau penerimaan tahunan

Sanksi administratif berupa denda administratif paling tinggi 2 (dua) persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

Penjatuhan sanksi administratif diberikan oleh Lembaga.

2

### Pendekatan Proaktif

Dengan adanya persyaratan baru yang signifikan dalam pemrosesan dan pemeliharaan data pribadi, diperlukan perekaman perjalanan data sebagai jejak audit.

Perusahaan harus memiliki pandangan yang proaktif dan komprehensif tentang data mereka dan mematuhi persyaratan yang ada di UU PDP.

3

### Data Protection Officer

Kebutuhan pasar yang meningkat terhadap spesialis independen

Perusahaan yang memproses data pribadi dalam skala besar diminta untuk menunjuk Pejabat/Petugas Pelindungan Data Pribadi yang independent dan berkualifikasi memadai.

Tantangan: Masih sedikitnya individu dengan keterampilan dan pengalaman yang memadai.

4

### Pemberitahuan & Persetujuan Privasi

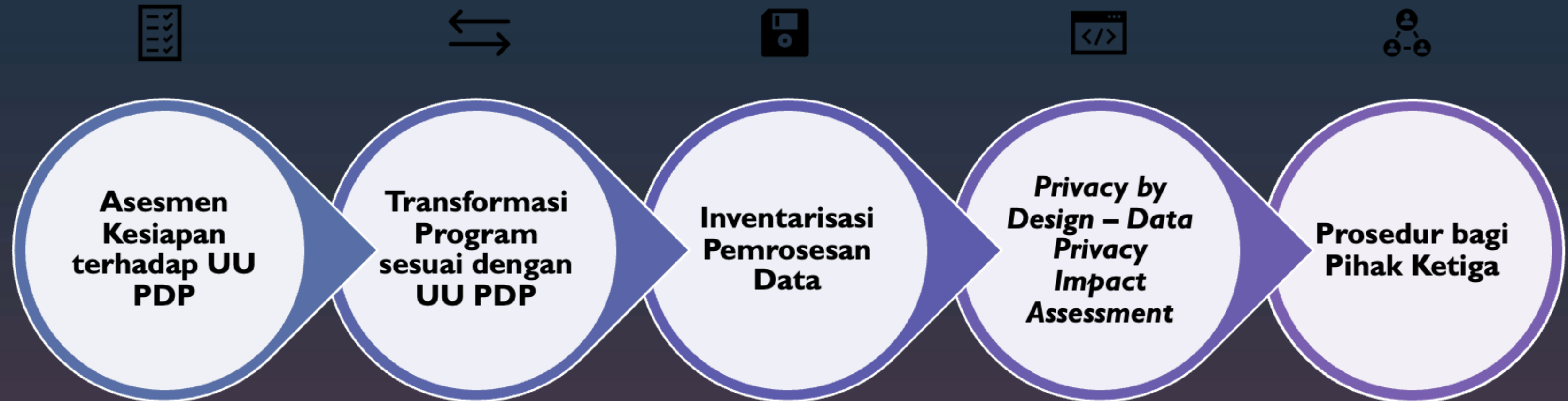
Penjelasan dan Edukasi adalah kuncinya

Organisasi harus mempertimbangkan dengan hati-hati dalam menyusun kebijakan privasi dan memberikan informasi yang lebih rinci.

UU PDP menekankan gagasan persetujuan sebagai salah satu syarat pemrosesan yang sah, perusahaan diwajibkan untuk mendapatkan persetujuan yang diberikan secara bebas, spesifik, diinformasikan, dan tidak ambigu. Kriteria tersebut wajib untuk dipenuhi.

# TINDAKAN YANG HARUS DIAMBIL

TINDAKAN YANG DIAMBIL UNTUK PERSIAPAN TERHADAP UU PDP



# ASESMEN KESIAPAN TERHADAP UU PDP



Jalan menuju kepatuhan terhadap  
UU PDP dengan Asesmen dan  
*Roadmap*



## Asesmen Kesiapan terhadap UU PDP

- Metodologi yang kuat berdasarkan praktik yang ada untuk membuat dasar untuk privasi.
- Bagian dari perangkat siber, yang berpotensi untuk dimasukkan ke dalam strategi dan *roadmap*.
- Digunakan secara global untuk penialai privasi dan siber.
- Titik awal yang baik untuk mematuhi UU PDP dan mendapatkan program privasi yang sesuai.
- Dilakukan berdasarkan kerangka kerja privasi, keamanan, dan tata kelola.
- Berperan dalam menemukan area dengan risiko terbesar
- Digunakan untuk fokus pada area yang paling membutuhkan tindakan sesuai dengan UU PDP.
- Metode untuk mengukur seberapa matang organisasi/perusahaan

## Langkah pertama untuk mematuhi UU PDP

Pendekatan asesmen didasarkan pada praktik di industri dengan tolok ukur privasi (*privacy benchmark*) dan tolok ukur tata kelola (*governance benchmark*), yang dapat dirujuk untuk menentukan posisi perusahaan terhadap UU PDP.

- **Wawasan Bisnis**

Kepatuhan privasi dan kerangka kerja kesiapan terhadap UU PDP yang disesuaikan berdasarkan karakteristik industri dan organisasi.

- **Wawasan dalam Situasi Privasi Saat Ini**

Penilaian menyeluruh dengan *workshop* dan wawancara dengan bagian dari perusahaan, memberikan wawasan tentang tingkatan kedewasaan saat ini terhadap kerangka kerja.

- **Pengembangan Strategi dan *Road Map***

*Road map* yang praktis dan konkret dengan langkah-langkah prioritas yang diperlukan untuk meningkatkan, berbasisrisiko, dan memuat status kepatuhan privasi terhadap UUPDP.

# PROSEDUR PIHAK KETIGA

---



## PROSEDUR PENANGANAN

### PELANGGARAN/KEGAGALAN DATA PRIBADI

Ketika terjadi pelanggaran data, ada banyak tantangan internal dan eksternal. Prosedur penanganan dan komunikasi dengan pemroses, otoritas, dan subjek data sangat penting untuk penanganan pelanggaran data yang efektif.



## PERJANJIAN PEMROSESAN DATA

Perjanjian pemrosesan data harus sesuai dengan ketentuan UU PDP. Dengan berlakunya aturan pelanggaran data baru, ada persyaratan untuk mengatur kontrak antara Pengendali dan Pemroses.



## PENILAIAN VENDOR

- Setiap kali perusahaan menggunakan pihak ketiga untuk segala jenis layanan yang mungkin melibatkan pemrosesan data, harus ada proses konkret dengan persyaratan yang jelas untuk menilai pihak tersebut dan layanan spesifik mereka.
- Perlu ada kolaborasi efektif antara hukum, penilai risiko, IT, dan pengadaan dengan arahan DPO.



## PROSEDUR HAK SUBJEK DATA PRIBADI

- Pemangku kepentingan eksternal yang paling penting adalah subjek data. Terdapat peningkatan hak untuk subjek data di UU PDP dan berpengaruh kepada prosedur oleh Pengendali.
- Subjek data dapat meminta akses mengoreksi, membatasi, mengajukan keberatan, atau penghapusan portabilitas data mereka. Sehingga proses yang baik tentang cara berkomunikasi dan melayani subjek data sangat penting.

# PRIVACY IMPACT ASSESSMENTS

## Apa itu?

Privacy Impact Assessment (PIA) adalah penilaian tertulis sebelumnya mengenai dampak operasi pemrosesan yang direncanakan terhadap perlindungan data pribadi. PIA memberikan cara berpikir terstruktur tentang risiko yang ditimbulkan pada orang-orang yang datanya diproses. PIA juga membantu mematuhi persyaratan perlindungan data yang telah diatur dalam UU PDP

## Mengapa PIA diperlukan?

- Untuk memahami dan memitigasi risiko terhadap hak-hak masyarakat
- Untuk mematuhi kewajiban hukum (Pasal 20 UU PDP )

## Apa saja yang harus disertakan dalam PIA?

- Deskripsi pengolahan yang direncanakan dan tujuannya
- Penilaian kebutuhan dan proporsionalitas
- Penilaian risiko terhadap subjek data
- Langkah-langkah untuk mengatasi risiko

## Siapa yang terlibat?

- Manajemen puncak (akuntabilitas)
- Pemilik bisnis
- DPO
- Departemen IT
- Prosesor

## Kapan itu wajib?

PIA adalah wajib untuk operasi pemrosesan data yang menghadirkan risiko tinggi terhadap data subjek seperti ketika dua kriteria berikut berlaku:

- Evaluasi/pembuatan profil yang sistematis
- Pengambilan keputusan otomatis
- Pemantauan sistematis
- Pemrosesan data sensitif
- Pemrosesan skala besar
- Cocokkan/gabungkan dataset dengan yang berbeda tujuan
- Subyek data yang rentan
- Teknologi baru
- Mencegah orang menjalankan haknya atau mengadakan suatu jasa/kontrak

# PRIVACY IMPACT ASSESSMENTS



Menanamkan privasi ke dalam metodologi proyek dengan menilai risiko privasi pada tahap awal.



## Pendekatan yang disesuaikan

- Privasi dapat dianggap sebagai risiko operasional yang memerlukan solusi praktis untuk memastikan bahwa risiko benar-benar ditangani.
- Tantangannya adalah menyediakan metodologi dan proses yang seragam dan fleksibel untuk menjaga privasi setiap kali proyek berbasis data dimulai.

## Elemen Penting

- Memastikan proyek dan inisiatif baru mematuhi aturan privasi.
- *DPIA* didasarkan pada Pasal 34 UU PDP dan merupakan alat yang efektif untuk menilai risiko privasi.

## Proses DPIA



# LANGKAH-LANGKAH PENYUSUNAN PIA

## 1 Identifikasi Cakupan PIA

Tentukan sistem informasi, proyek, atau inisiatif yang akan menjadi subjek PIA.

## 1 Identifikasi Pemangku Kepentingan

Identifikasi individu atau kelompok yang akan terpengaruh oleh sistem informasi, proyek, atau inisiatif.

## 1 Identifikasi Informasi Identitas Pribadi (PII)

Identifikasi jenis PII yang akan dikumpulkan, digunakan, disimpan, atau dibagikan.

## 1 Lakukan Penilaian Risiko Privasi

Identifikasi dan nilai risiko privasi yang terkait dengan pengumpulan, penggunaan, penyimpanan, dan pembagian PII.

## 1 Identifikasi Kontrol Privasi

Identifikasi dan evaluasi proses alternatif untuk menangani informasi untuk mengurangi potensi risiko privasi.

## 1 Dokumentasikan PIA

Dokumentasikan proses dan hasil analisis dalam dokumen resmi.