Universitas
Bina Sarana Informatika

MODUL PENDAMPING

PELATIHAN PENINGKATAN KESADARAN PELINDUNGAN DATA PRIBADI UNTUK PENCEGAHAN KEJAHATAN SIBER DI LEMBAGA PENDIDIKAN RA DAARUL FIKRI

2026

Silabus Kebijakan & Agenda Pelatihan

Pengantar

Modul ini dirancang secara komprehensif untuk menjadi panduan akademis sekaligus praktis dalam memahami regulasi pelindungan data pribadi (PDP). Materi yang disajikan mencakup fondasi teoretis, komparasi standar internasional, pembahasan detail pasal demi pasal UU PDP No. 27/2022, hingga implementasi praktis dan studi kasus nyata.

1. Modul I: Fondasi Utama, Urgensi Kebijakan, dan Konsekuensi Pelanggaran Privasi Data
2. Modul II: Landasan Global Teoretis (GDPR, ISO 27701, NIST Privacy Framework)
3. Modul III: Analisis Gap Komparatif Antara Regulasi Internasional dan Undang-Undang PDP
4. Modul IV: Kerangka Konseptual, Definisi Komprehensif, dan Kategorisasi Data Menurut UU PDP
5. Modul V: Asas Pemrosesan Hukum (Lawful Basis) dan Batasan Yurisdiksi Hukum Perlindungan Data
6. Modul VI: Struktur Aktor Kelembagaan (Subjek Data, Pengendali Data, dan Prosesor Data)
7. Modul VII: Sembilan Prinsip Baku Tata Kelola Pelindungan Data Pribadi Kontemporer
8. Modul VIII: Hak-Hak Konstitusional Subjek Data dan Tata Cara Penyelesaian Sengketa Privasi
9. Modul IX: Kewajiban Hukum, Teknis, dan Operasional Pengendali Data Pribadi
10. Modul X: Kewajiban Khusus Pemrosesan Data Anak-Anak dan Penyandang Disabilitas
11. Modul XI: Instrumen Manajemen Risiko: Data Protection Impact Assessment (DPIA)

12. Modul XII: Prinsip Arsitektur Teknologi: Data Protection by Design dan by Default
13. Modul XIII: Mekanisme Penanganan Keadaan Darurat Kebocoran Data (Data Breach Notification)
14. Modul XIV: Peran, Kualifikasi, Fungsi Kebijakan, dan Tugas Data Protection Officer (DPO)
15. Modul XV: Kelembagaan Otoritas Pengawas Independen Perlindungan Data Pribadi
16. Modul XVI: Kerangka Regulasi Penegakan Hukum: Sanksi Administratif Organisasional
17. Modul XVII: Kerangka Regulasi Penegakan Hukum: Ketentuan Sanksi Pidana Korporasi dan Individu
18. Modul XVIII: Kajian Kasus Kebocoran Data Global Kontemporer (Facebook & Cambridge Analytica)
19. Modul XIX: Kajian Kasus Pola Desain Manipulatif (Dark Patterns) Aplikasi Temu
20. Modul XX: Kajian Kasus Pelanggaran Regulasi Sektoral Uni Eropa (Analisis Kasus Meta, Amazon, TikTok)
21. Modul XXI: Panduan Audit Kepatuhan, Evaluasi Kesiapan Mandiri, dan Penyusunan Peta Risiko Internal
22. Modul XXII: Langkah Strategis Implementasi Tata Kelola Kepatuhan Berkelanjutan di Lembaga Pendidikan

Modul I: Urgensi Kebijakan dan Konsekuensi Pelanggaran Privasi Data

1.1 Latar Belakang dan Urgensi Kesadaran Privasi

Di era transformasi digital yang masif, data telah menjelma menjadi komoditas baru yang bernilai sangat tinggi (data is the new oil). Bagi lembaga pendidikan seperti RA Daarul Fikri, pengumpulan data murid, orang tua, dan staf pengajar merupakan aktivitas harian. Namun, tanpa adanya kesadaran hukum (privacy awareness) dan tata kelola yang memadai, data pribadi tersebut sangat rentan disalahgunakan oleh pelaku kejahatan siber.

1.2 Dampak Katastropik Kebocoran Data

Kebocoran data pribadi bukan sekadar permasalahan teknis kebocoran sistem informasi, melainkan ancaman multidimensional yang dapat melumpuhkan eksistensi sebuah lembaga. Terdapat lima pilar konsekuensi fatal jika aspek privasi diabaikan:

1. Kerusakan reputasi institusi (Reputational Damage) yang mengakibatkan hilangnya kepercayaan publik, orang tua siswa, dan mitra strategis secara permanen.
2. Kerugian finansial (Financial Loss) akibat biaya pemulihan sistem, investigasi forensik digital, denda administratif regulasi, hingga gugatan ganti rugi perdata.
3. Tuntutan hukum dan sanksi pidana (Legal Penalties) bagi pengurus yayasan atau manajemen organisasi akibat kelalaian tata kelola data.
4. Ancaman keselamatan fisik dan psikis bagi individu (Subjek Data), seperti maraknya kejahatan siber berupa penipuan berbasis rekayasa sosial (social engineering), pemerasan, hingga intimidasi oleh penyedia pinjaman online ilegal.
5. Kehilangan keunggulan kompetitif organisasi dan pudarnya integritas institusi di mata hukum.

Modul II: Landasan Global Teoretis (GDPR, ISO 27701, NIST Framework)

2.1 General Data Protection Regulation (GDPR)

GDPR yang disahkan oleh Uni Eropa pada tahun 2016 dan berlaku efektif pada Mei 2018 merupakan regulasi privasi paling ketat dan berpengaruh di dunia. Regulasi ini mengubah paradigma perlindungan data global dengan menetapkan hak-hak individu yang kuat dan memberikan sanksi denda yang sangat tinggi guna memastikan korporasi global memperlakukan data pribadi dengan rasa hormat.

2.2 ISO/IEC 27701: Standar Manajemen Privasi Internasional

ISO/IEC 27701 merupakan standar sertifikasi internasional yang memberikan panduan terperinci untuk membangun, menerapkan, memelihara, dan secara terus-menerus meningkatkan Privacy Information Management System (PIMS). Standar ini merupakan ekstensi langsung dari ISO/IEC 27001 (Manajemen Keamanan Informasi), memastikan bahwa privasi diintegrasikan ke dalam tata kelola keamanan informasi organisasi secara holistik.

2.3 NIST Privacy Framework: Pendekatan Manajemen Risiko berbasis Hasil

Dikembangkan oleh National Institute of Standards and Technology (NIST) Amerika Serikat, framework ini menyediakan alat bantu sukarela yang fleksibel bagi organisasi untuk mengelola risiko privasi. Pendekatan NIST berfokus pada mitigasi konsekuensi buruk dari pemrosesan data terhadap individu melalui sistem yang adaptif dan berbasis pada hasil perlindungan nyata.

Modul III: Analisis Gap Regulasi Internasional vs UU PDP

3.1 Tabel Matriks Analisis Karakteristik Regulasi Global

Kriteria / Regulasi	Yurisdiksi & Asal	Sifat Kepatuhan	Fokus Utama Tata Kelola
GDPR	Uni Eropa (Berlaku Global via Ekstrateritorial)	Wajib (Mandatory Hukum)	Perlindungan hak fundamental privasi warga Uni Eropa.
ISO 27701	Internasional (ISO/IEC)	Sukarela (Voluntary Sertifikasi)	Standarisasi sistem manajemen informasi privasi internal.
NIST Framework	Amerika Serikat (NIST)	Sukarela (Voluntary Praktik)	Pengelolaan risiko privasi melalui siklus hidup data.
UU PDP No. 27/2022	Indonesia	Wajib (Mandatory Hukum)	Kedaulatan dan perlindungan data pribadi nasional.

3.2 Analisis Celah Kepatuhan (Gap Analysis) Struktural

Meskipun UU PDP mengadopsi banyak prinsip GDPR, terdapat celah kepatuhan operasional mendasar yang wajib dipahami:

1. Ketepatan Waktu Notifikasi Kebocoran: UU PDP menetapkan batas kaku 3 x 24 jam untuk laporan resmi (Pasal 46), sementara GDPR memberikan kelonggaran hingga 72 jam jika terdapat alasan logis penundaan.
2. Kualifikasi Data Protection Officer (DPO): UU PDP mensyaratkan penunjukan berdasarkan kapasitas hukum domestik yang jelas untuk sektor publik dan skala

besar, sedangkan ISO 27701 menaruh fokus pada kompetensi operasional manajerial tanpa ikatan yurisdiksi.

3. Ancaman Sanksi Pidana: UU PDP secara tegas memuat ancaman kurungan penjara fisik hingga denda korporasi 10 kali lipat bagi pelaku pelanggaran (Pasal 67-73). Sebaliknya, GDPR murni mengandalkan sanksi administratif finansial, dan standar ISO tidak memiliki kekuatan hukum pemidanaan.

Modul IV: Kerangka Konseptual dan Kategorisasi Data Menurut UU PDP

4.1 Definisi Hukum Perlindungan Data Pribadi

Berdasarkan ketentuan umum UU PDP No. 27/2022 Pasal 1, Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.

4.2 Kategorisasi Data Pribadi Berdasarkan Tingkat Risiko

Undang-undang membagi data pribadi ke dalam dua kelompok besar yang berimplikasi langsung pada tingkat pengamanan teknis yang wajib diterapkan:

1. Data Pribadi yang Bersifat Spesifik (Sensitif): Meliputi data kesehatan, data biometrik, data genetika, catatan kejahatan, data anak-anak, data keuangan pribadi, dan data lainnya yang jika bocor dapat membahayakan keamanan, diskriminasi, atau kerugian material yang besar bagi pemiliknya.
2. Data Pribadi yang Bersifat Umum: Meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Modul V: Asas Pemrosesan Hukum (Lawful Basis) dan Batasan Yurisdiksi

5.1 Enam Asas Keabsahan Pemrosesan Data (Lawful Basis)

Pengendali data dilarang keras mengumpulkan atau memproses data tanpa memiliki salah satu dari enam dasar hukum yang sah berikut:

1. Persetujuan yang sah secara eksplisit (Consent) dari subjek data untuk satu atau beberapa tujuan tertentu yang telah diinformasikan secara jelas.
2. Pemenuhan kewajiban perjanjian/kontrak (Contractual Necessity) di mana subjek data merupakan salah satu pihak.
3. Pemenuhan kewajiban hukum (Legal Obligation) pengendali data berdasarkan peraturan perundang-undangan.
4. Pemenuhan perlindungan kepentingan vital (Vital Interest) dari subjek data demi keselamatan jiwanya.
5. Pelaksanaan tugas dalam rangka kepentingan umum atau pelayanan publik (Public Necessity) berdasarkan hukum.
6. Pemenuhan kepentingan sah lainnya (Legitimate Interest) dengan memperhatikan keseimbangan antara kepentingan pengendali data dan hak-hak subjek data.

5.2 Ekstrateritorialitas dan Asas Asas Ekstra-Yurisdiksi

UU PDP menganut asas ekstrateritorialitas yang luas. Regulasi ini berlaku untuk setiap orang, badan hukum, badan publik, dan organisasi internasional yang melakukan perbuatan hukum di dalam yurisdiksi Indonesia, serta di luar yurisdiksi Indonesia selama perbuatan tersebut memiliki akibat hukum di dalam wilayah Indonesia atau merugikan subjek data warga negara Indonesia.

Modul VI: Struktur Aktor Kelembagaan Perlindungan Data

6.1 Trias Aktor Tata Kelola Data

Keberhasilan implementasi perlindungan data bersandar pada kejelasan fungsi dan tanggung jawab tiga aktor utama berikut:

1. **Aktor 1:** Subjek Data Pribadi: Orang perseorangan yang pada dirinya melekat data pribadi tertentu yang wajib dilindungi hak privasinya.
2. **Aktor 2:** Pengendali Data Pribadi (Data Controller): Pihak (perorangan, korporasi, badan publik) yang menentukan tujuan pemrosesan dan memegang kendali penuh atas keputusan pemrosesan data.
3. **Aktor 3:** Prosesor Data Pribadi (Data Processor): Pihak yang melakukan pemrosesan data pribadi atas nama, di bawah kendali, dan berdasarkan instruksi tertulis khusus dari Pengendali Data.

6.2 Batasan Relasi Kontraktual

Apabila Pengendali Data menunjuk Prosesor Data (misalnya lembaga pendidikan menggunakan vendor aplikasi absensi online pihak ketiga), seluruh kewajiban perlindungan data wajib dituangkan dalam kontrak hukum formal yang mengikat. Kegagalan pemrosesan oleh Prosesor tetap dapat memicu tanggung jawab hukum bagi Pengendali jika tidak diawasi dengan ketat.

Modul VII: Sembilan Prinsip Baku Tata Kelola Pelindungan Data

Prinsip perlindungan data merupakan ruh utama dari undang-undang ini yang wajib menjiwai setiap siklus hidup pengelolaan data, mulai dari perolehan hingga pemusnahan:

1. **Keterbatasan dan Legalitas:** Pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, serta transparan.
2. **Kesesuaian Tujuan:** Pemrosesan data pribadi dilakukan sesuai dengan tujuan pemrosesan yang telah disampaikan secara eksplisit.
3. **Pemenuhan Hak:** Pemrosesan dilakukan dengan menjamin hak-hak subjek data sesuai regulasi.
4. **Keakuratan Data:** Data pribadi yang diproses harus akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan.
5. **Keamanan Sistem:** Pemrosesan dilakukan dengan mengamankan dan melindungi data dari akses ilegal, pengubahan, atau kebocoran.
6. **Keterbukaan Informasi:** Adanya keterbukaan mengenai tujuan, aktivitas pemrosesan, dan kegagalan perlindungan data.
7. **Pembatasan Retensi:** Data pribadi dimusnahkan atau dihapus setelah masa retensi berakhir atau tujuan tercapai.
8. **Akuntabilitas Pengendali:** Seluruh aktivitas pemrosesan wajib dapat dibuktikan kepatuhannya secara akuntabel.
9. **Keselarasan Kepentingan:** Penggunaan data tidak boleh merugikan kepentingan pertahanan, keamanan nasional, dan hak publik yang sah.

Modul VIII: Hak-Hak Konstitusional Subjek Data & Sengketa

8.1 Manifestasi Hak-Hak Subjek Data

UU PDP memberikan kedaulatan penuh kepada individu atas datanya melalui hak-hak konstitusional berikut (Pasal 5 s.d. Pasal 13):

1. Hak kejelasan identitas, dasar kepentingan hukum, tujuan permintaan, dan akuntabilitas pihak yang meminta data.
2. Hak melengkapi, memperbarui, dan memperbaiki kesalahan atau ketidakakuratan data pribadi miliknya.
3. Hak mengakses dan memperoleh salinan data pribadi miliknya sesuai dengan rekam jejak pemrosesan.
4. Hak mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi miliknya.
5. Hak menarik kembali persetujuan (withdraw consent) yang telah diberikan tanpa penjelasan rumit.
6. Hak menolak keputusan yang sepenuhnya didasarkan pada pemrosesan otomatis (automated profiling).
7. Hak menunda atau membatasi pemrosesan data secara proporsional.
8. Hak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi miliknya.
9. Hak mentransfer data miliknya ke pengendali data lain dalam format yang terbaca sistem (Data Portability).

8.2 Hukum Acara Penyelesaian Sengketa Privasi

Subjek data yang haknya dilanggar dapat mengajukan pengaduan resmi kepada Otoritas Pengawas. Sengketa privasi dapat diselesaikan melalui lembaga alternatif penyelesaian sengketa atau arbitrase, tanpa menutup hak subjek data untuk mengajukan gugatan perdata ke pengadilan negeri atas kerugian immaterial dan material yang diderita.

Modul IX: Kewajiban Hukum, Teknis, dan Operasional Pengendali Data

9.1 Kewajiban Akuntabilitas Administratif

Pengendali Data memiliki tanggung jawab hukum mutlak dalam membuktikan kepatuhan (burden of proof). Kewajiban operasional utama meliputi:

1. Wajib memiliki dasar hukum yang sah (lawful basis) sebelum memulai pemrosesan.
2. Wajib menyampaikan informasi identitas, tujuan pemrosesan, dan hak-hak subjek data secara berkala dan transparan.
3. Wajib melakukan perekaman seluruh aktivitas pemrosesan data pribadi (Record of Processing Activities / RoPA).

9.2 Kewajiban Pengamanan Teknis Siber

Secara teknis, Pengendali wajib menerapkan langkah pengamanan tingkat tinggi untuk mencegah insiden siber:

1. Menerapkan enkripsi data pada saat data disimpan (data-at-rest) maupun saat ditransmisikan (data-in-transit).
2. Membangun sistem pembatasan hak akses kontrol yang ketat (Role-Based Access Control) sehingga data hanya dapat diakses staf yang berwenang.
3. Melakukan uji kerentanan keamanan informasi secara berkala (Penetration Testing).

Modul X: Kewajiban Khusus Pemrosesan Data Anak & Disabilitas

10.1 Perlindungan Berlapis Data Anak-Anak

Dalam konteks lembaga pendidikan seperti RA (Raudhatul Athfal) Daarul Fikri, pemrosesan data anak di bawah umur merupakan aktivitas inti. UU PDP Pasal 25 menegaskan bahwa pemrosesan data pribadi anak wajib diselenggarakan secara khusus, mendapat perlindungan ekstra, dan wajib memperoleh persetujuan tertulis (consent) dari orang tua dan/atau wali sah anak yang bersangkutan.

10.2 Pemrosesan Data Penyandang Disabilitas

Sama halnya dengan data anak, pemrosesan data pribadi bagi penyandang disabilitas memerlukan perhatian khusus. Pengendali data wajib menyediakan mekanisme komunikasi yang aksesibel, ramah disabilitas, dan memperoleh persetujuan melalui wali hukum yang sah untuk memastikan hak-hak privasi mereka tidak terdiskriminasi.

Modul XI: Instrumen Manajemen Risiko: Data Protection Impact Assessment

11.1 Definisi dan Kriteria Wajib DPIA

Data Protection Impact Assessment (DPIA) atau Penilaian Dampak Pelindungan Data adalah proses sistematis untuk menganalisis pemrosesan data guna mengidentifikasi dan meminimalkan risiko privasi. Sesuai Pasal 34, Pengendali Data WAJIB melakukan DPIA jika pemrosesan berpotensi menghasilkan risiko tinggi terhadap subjek data.

11.2 Skenario Pemrosesan Berisiko Tinggi

1. Pemrosesan data pribadi spesifik (sensitif) seperti rekam medis, data biometrik, atau rekam jejak kriminal dalam skala besar.
2. Evaluasi atau penilaian profil individu secara sistematis dan meluas (automated profiling/scoring).
3. Pengawasan massal secara meluas pada area publik, misalnya penggunaan CCTV pintar berbasis pengenalan wajah (facial recognition).
4. Penggunaan teknologi baru yang belum umum digunakan dan memiliki dampak siber yang belum dipetakan penuh.

Modul XII: Prinsip Arsitektur: Data Protection by Design & by Default

12.1 Data Protection by Design

Prinsip ini mengharuskan organisasi untuk mengintegrasikan perlindungan data dan pertimbangan privasi ke dalam setiap tahap siklus pengembangan sistem, produk aplikasi, proses bisnis, atau infrastruktur IT sejak awal perencanaan, bukan sebagai komponen pelengkap (*add-on*) di akhir proyek.

12.2 Data Protection by Default

Prinsip ini memastikan bahwa setelan bawaan (*default settings*) pada aplikasi atau sistem secara otomatis menerapkan perlindungan privasi yang maksimal tanpa memerlukan tindakan manual dari pengguna. Contoh nyata: penutupan opsi pembagian data ke pihak ketiga secara otomatis saat akun pertama kali dibuat, serta pembatasan pengumpulan data seminimal mungkin yang diperlukan untuk menjalankan fungsi utama sistem (*data minimization*).

Modul XIII: Mekanisme Penanganan Kebocoran Data (Breach Notification)

13.1 Kewajiban Notifikasi Kilat 3 x 24 Jam

Dalam hal terjadi kegagalan pelindungan data pribadi (data breach), Pengendali Data wajib bergerak cepat tanpa penundaan. Pasal 46 ayat (1) menegaskan bahwa Pengendali wajib menyampaikan pemberitahuan tertulis maksimal dalam waktu 3 x 24 jam kepada Subjek Data Pribadi dan Otoritas Pengawas.

13.2 Komponen Wajib Isi Notifikasi Kebocoran

Pemberitahuan tertulis kebocoran data wajib memuat sekurang-kurangnya informasi berikut guna meminimalkan dampak keparahan:

1. Kronologi detail mengenai kapan dan bagaimana kegagalan sistem keamanan data terjadi.
2. Kategorisasi dan perkiraan jumlah data pribadi yang terungkap atau bocor.
3. Upaya penanganan, mitigasi risiko siber, dan pemulihan sistem yang telah dan sedang diupayakan oleh organisasi.
4. Rekomendasi langkah penyelamatan mandiri yang dapat segera dilakukan oleh subjek data (misalnya penggantian kata sandi dan pengaktifan 2FA).

Modul XIV: Peran, Fungsi, dan Tugas Data Protection Officer (DPO)

14.1 Kriteria Mandat Penunjukan DPO

Pasal 53 menetapkan bahwa Pengendali Data dan Prosesor Data wajib menunjuk Pejabat atau Petugas Pelindung Data (Data Protection Officer / DPO) dalam hal:

1. Pemrosesan data pribadi dilakukan untuk kepentingan pelayanan publik atau badan publik.
2. Kegiatan utama pengendali data memerlukan pengawasan teratur dan sistematis terhadap subjek data dalam skala besar.
3. Kegiatan utama pengendali data berfokus pada pemrosesan data pribadi yang bersifat spesifik (sensitif) skala besar.

14.2 Tugas Pokok dan Independensi DPO

DPO bertindak sebagai jembatan kepatuhan independen yang bertugas menginformasikan dan memberikan saran kepada manajemen mengenai kewajiban hukum PDP, memantau kepatuhan internal terhadap undang-undang, serta menjadi titik kontak utama bagi subjek data dan Otoritas Pengawas.

Modul XV: Kelembagaan Otoritas Pengawas Perlindungan Data

15.1 Kedudukan Kebijakan Kelembagaan

UU PDP mengamanatkan pembentukan Otoritas Pengawas Perlindungan Data Pribadi yang ditetapkan oleh Presiden dan bertanggung jawab langsung kepada Kepala Negara. Lembaga ini bertindak sebagai regulator independen yang memegang kendali penuh atas penegakan hukum privasi di wilayah kedaulatan digital Indonesia.

15.2 Wewenang Eksekutif Otoritas Pengawas

Otoritas memiliki wewenang yang luas untuk menjaga marwah undang-undang, antara lain:

1. Merumuskan kebijakan teknis operasional perlindungan data pribadi nasional.
2. Melakukan pengawasan kepatuhan, audit independen, serta investigasi forensik digital atas dugaan pelanggaran privasi.
3. Menerima pengaduan masyarakat, menjatuhkan sanksi administratif, dan bertindak sebagai mediator penyelesaian sengketa.

Modul XVI: Kerangka Sanksi Administratif Organisasional

16.1 Spektrum Sanksi Administratif Non-Moneter

Bagi instansi atau korporasi yang melanggar ketentuan tata kelola data tetapi tidak memenuhi unsur pidana, Otoritas Pengawas dapat menjatuhkan sanksi bertingkat sesuai Pasal 57:

1. Peringatan tertulis resmi sebagai teguran awal agar organisasi melakukan perbaikan.
2. Penghentian sementara seluruh aktivitas pemrosesan data pribadi untuk membatasi risiko perluasan kebocoran.
3. Perintah penghapusan atau pemusnahan total data pribadi yang dikelola secara ilegal.

16.2 Sanksi Administratif Finansial (Denda Fiskal)

Selain sanksi non-moneter, undang-undang menetapkan sanksi denda administratif yang sangat signifikan, yaitu maksimal sebesar 2% (dua persen) dari total pendapatan tahunan atau omzet tahunan organisasi terhadap variabel pelanggaran tertentu.

Modul XVII: Kerangka Sanksi Pidana Korporasi dan Individu

17.1 Delik Pidana Individu (Pasal 67 s.d. Pasal 69)

UU PDP memuat ketentuan pemidanaan yang sangat tegas bagi pelaku kejahatan siber berbasis data pribadi:

1. Setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain dipidana penjara maksimal 5 tahun dan/atau denda maksimal Rp5 Miliar.
2. Setiap orang yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya dipidana penjara maksimal 4 tahun dan/atau denda maksimal Rp4 Miliar.
3. Setiap orang yang dengan sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya dipidana penjara maksimal 5 tahun dan/atau denda maksimal Rp5 Miliar.
4. Setiap orang yang dengan sengaja memalsukan data pribadi untuk menguntungkan diri sendiri dipidana penjara maksimal 6 tahun dan/atau denda maksimal Rp6 Miliar.

17.2 Pertanggungjawaban Pidana Korporasi (Corporate Liability)

Apabila tindak pidana dilakukan oleh korporasi atau badan usaha, pidana dapat dijatuhkan kepada pengurus, pemegang kendali, atau korporasi itu sendiri. Denda bagi korporasi dapat dijatuhkan hingga 10 kali lipat dari batas maksimal denda individu, disertai sanksi tambahan berupa pembekuan usaha, pencabutan izin, hingga pembubaran badan hukum.

Modul XVIII: Studi Kasus Global: Facebook & Cambridge Analytica

18.1 Anatomi dan Kronologi Kasus

Pada tahun 2018, dunia diguncang oleh skandal penyalahgunaan data profil pengguna Facebook oleh firma konsultan politik Cambridge Analytica. Data dari 87 juta pengguna dikumpulkan secara ilegal melalui aplikasi kuesioner kepribadian pihak ketiga ('This is Your Digital Life') tanpa persetujuan eksplisit pemilik data.

18.2 Pemanfaatan Data dan Pembelajaran Regulasi

Data yang dikumpulkan dikonversi menjadi profil psikografis untuk menyusun strategi kampanye politik *microtargeting* yang manipulatif pada Pemilu Presiden AS 2016. Kasus ini menjadi katalisator global yang membuktikan betapa berbahayanya eksploitasi data privasi terhadap demokrasi, mempercepat implementasi GDPR di Eropa, dan menginspirasi lahirnya UU PDP di berbagai negara, termasuk Indonesia.

Modul XIX: Studi Kasus Pola Desain Manipulatif Aplikasi Temu

19.1 Dark Patterns dan Akses Data Invasif

Aplikasi *e-commerce* global Temu menghadapi pengawasan ketat dan gugatan hukum berat karena menerapkan pola desain antarmuka yang manipulatif (*dark patterns*). Antarmuka aplikasi dirancang sedemikian rupa untuk menjebak pengguna agar memberikan izin akses data yang melampaui batas kewajaran fungsi belanja daring.

19.2 Eksploitasi Hak Akses Perangkat Sistem

Aplikasi ini terindikasi menguras data sensitif perangkat pengguna secara invasif, termasuk pelacakan lokasi presisi secara terus-menerus, akses penuh ke kamera, mikrofon, riwayat SMS, dokumen penyimpanan internal, hingga enkripsi biometrik sidik jari. Kasus ini membuktikan pelanggaran nyata terhadap prinsip minimisasi data (*data minimization*) kontemporer.

Modul XX: Rangkuman Kasus Pelanggaran Regulasi GDPR di Uni Eropa

Penegakan hukum internasional melalui GDPR memberikan potret nyata mengenai ketegasan denda finansial bagi organisasi yang mengabaikan privasi data:

No	Perusahaan & Nilai Denda	Otoritas Pengawas	Inti Pelanggaran Regulasi & Kegagalan
1	Meta (2023) €1.2 Miliar	Ireland DPC	Melakukan transfer data pengguna Eropa ke server Amerika Serikat tanpa jaminan keamanan setara.
2	Amazon (2021) €746 Juta	Luxembourg CNDP	Mengeksploitasi data riwayat pencarian pengguna untuk iklan tanpa persetujuan sah.
3	Meta (2022) €405 Juta	Ireland DPC	Pengaturan default akun Instagram anak tersetel publik secara otomatis, mengekspos kontak pribadi.
4	TikTok (2023) €345 Juta	Ireland DPC	Mekanisme verifikasi usia yang lemah dan memproses data anak tanpa batas pelindung.
5	H&M (2020) €35.25 Juta	Hamburg BfDI	Mengumpulkan data latar belakang pribadi dan keluarga karyawan secara ilegal untuk evaluasi kinerja.

Modul XXI: Panduan Audit Kepatuhan & Peta Risiko Internal

21.1 Pemetaan Aliran Data (Data Mapping)

Langkah pertama menuju kepatuhan UU PDP adalah melakukan audit internal dengan memetakan seluruh siklus hidup data. Organisasi wajib menjawab secara tertulis: Data apa saja yang dikumpulkan? Di mana data tersebut disimpan? Siapa saja yang memiliki hak akses? Bagaimana metode transfernya? Dan kapan data tersebut harus dimusnahkan?

21.2 Penyusunan Formulir Kesiapan Mandiri (Gap Analysis)

Organisasi wajib menyusun instrumen evaluasi mandiri (*self-assessment*) untuk menilai kesenjangan operasional internal terhadap 9 prinsip dasar UU PDP, mengidentifikasi kerentanan sistem TI, serta menyusun Dokumen Registrasi Risiko Privasi untuk memitigasi kemungkinan terjadinya insiden kebocoran data siber.

Modul XXII: Langkah Strategis Tata Kelola di Lembaga Pendidikan

22.1 Rencana Kepatuhan Operasional Berkelanjutan

Untuk menindaklanjuti pelatihan pengabdian kepada masyarakat ini, RA Daarul Fikri direkomendasikan menyusun cetak biru (*blueprint*) kepatuhan operasional jangka pendek dan menengah:

1. **Langkah 1:** Pembaruan Formulir Persetujuan (Consent Form) Pendaftaran Siswa Baru dengan mencantumkan tujuan penggunaan data secara spesifik dan klausul persetujuan tertulis orang tua.
2. **Langkah 2:** Penyusunan SOP Penanganan Insiden Kebocoran Data Internal agar staf tahu ke mana harus melapor dalam waktu 3 x 24 jam jika terjadi kegagalan sistem.
3. **Langkah 3:** Penerapan pembatasan akses data fisik (berkas formulir di lemari terkunci) dan data digital (kata sandi komputer admin dan pengaktifan enkripsi flashdisk penyimpan data).
4. **Langkah 4:** Pelaksanaan program edukasi dan pelatihan penyegaran berkala bagi guru dan staf tata usaha demi menjaga budaya sadar privasi (*privacy-aware culture*).

22.2 Penutup: Komitmen Bersama

Kesimpulan Akhir: Pelindungan data pribadi bukanlah program kerja teknologi informasi yang bersifat sementara, melainkan komitmen kepatuhan hukum dan etis yang berkelanjutan. Menjaga data anak didik kita di RA Daarul Fikri berarti melindungi masa depan mereka dan menjaga integritas institusi dari ancaman kejahatan siber.

"Menjaga keamanan data pribadi anak-anak di lingkungan pendidikan usia dini adalah pondasi untuk melindungi masa depan mereka, memanfaatkan teknologi dengan bijak, dan meningkatkan kesadaran akan pentingnya privasi sejak dini."

Dari UBSI untuk Negeri

ADE SURYA BUDIMAN, S.T., M.KOM (0326028202)
ERWIN SETYAWAN, S.T., M.PD. (0326098305)
NUR ALI FARABI, M.KOM (0406077502)
FAHRIZAL, S.PD., M.KOM (0301048303)
AHMAD SYAMSI ASHARI (15240440)
NAUFAL HARYADI (15220605)