WEBINAR SERIES
BY xynexis

Privacy Day Special Edition
28 Jan 2026

Satriyo W — Narasumber
Santun — Moderator

PDP 2026:
Siap Audit
atau Berisiko Sanksi?

Roadmap Operasional & Checklist Wajib Pemimpin IT

SATRIYO WIBOWO S.T., MBA, M.H., IPM | **CCISO**, CBP, CSA, **ECIH, CEH** |
Fellow of Information Privacy, AIGP, **CIPP**/A/C/**E**/**US, CIPM, CIPT**|
GRCP, GRCA, IPMP, IDPP, IAIP, IRMP

- Asia Advisory Board - IAPP
- Lead Data Protection Consultant PT Xynexis International
- Board Secretary Indonesia Cyber Security Forum
- Asosiasi Forensik Digital Indonesia
- Narasumber Teknis Penomoran Internet Dir. Telekomunikasi PPI Kominfo, Wantannas, IoT/5G Dir. Standardisasi SDPPI, Tenaga ahli KEIN dan DEN, SDM Kamsibersandi BSSN
- Tim perumus Peta Okupasi TIK, Kamsiber, dan PDP
- Anggota tim perumus SKKNI SOC, Digital Forensik, Audit Keamanan Informasi, Uji Keamanan Siber, Kriptografi, Keamanan Informasi (revisi), Kesadaran Keamanan Informasi, Tanggap Insiden Siber
- Ketua Tim Perumus SKKNI Pelindungan Data Pribadi
- Anggota Komtek 35-04 BSN menangani Keamanan Informasi, Keamanan Siber, dan Pelindungan Privasi, Ketua GK5 – Manajemen Identitas dan Teknologi Privasi
- IVLP 2019 on Cybersecurity Policy Development and Implementation

Rekap Materi PDP sejak 2020

https://www.linkedin.com/in/swibowo/

Ringkasan

Agenda Eksekutif

01 **Konteks Global**

Privasi sebagai "License to Operate" baru di 2026.

02 **Realitas Penegakan**

Navigasi transisi dari masa tenggang ke audit aktif.

03 **Roadmap 4-Pilar**

Pendekatan struktural untuk kepatuhan berkelanjutan.

04 **Model Kematangan**

Bergerak dari "Checklist" ke "Keunggulan Operasional".

05 **Langkah Selanjutnya**

Memulai Diagnostik Kesiapan 2026 Anda.

Konteks Strategis

2026: Titik Tidak Kembali

Dari "Kebijakan" ke "Bukti"

Regulator tidak lagi bertanya apakah Anda punya kebijakan; mereka meminta **bukti eksekusi** nyata.

Kepercayaan = Pendapatan

75% perusahaan B2B kini mewajibkan bukti kepatuhan PDP sebelum menandatangani kontrak.

Cakrawala Sanksi

Risiko bukan hanya denda, tapi **Penghentian Pemrosesan Data**—efektif mematikan bisnis.

Waktu Habis

Akhir Masa Transisi

Timeline Penegakan Hukum

2022–2024

Adaptasi Sukarela

Fase adaptasi dan kesadaran. Organisasi mulai mengenal UU PDP tanpa risiko sanksi langsung.

2025

Transisi & Peringatan

Penegakan lunak (soft enforcement). Peringatan administratif mulai diberikan.

2026

Siklus Penegakan Penuh

- ✓ Audit Regulasi Acak
- ✓ Tanggung Jawab Mutlak (Strict Liability)
- ✓ Wajib Lapor Insiden 72 Jam

Standar 2026

Normal Baru Akuntabilitas

Kedaulatan Data

Mengetahui secara pasti di mana data Anda berada (Cloud, On-Prem, Pihak Ketiga).

Kepatuhan Terbukti

Memelihara "File Manajemen Privasi" yang siap audit 24/7, bukan sekadar dokumen statis.

Otomasi Hak Subjek Data Pribadi

Bisakah tim IT Anda memenuhi permintaan "Penghapusan Data" dalam waktu 48 jam atau hak ”Penarikan Persetujuan”?

Reality Check

Tantangan Implementasi di Indonesia

DPO "Di Atas Kertas"

Menunjuk Data Protection Officer yang tidak memiliki **alat teknis** atau **wewenang hukum** untuk bertindak.

Krisis Shadow Data

PII (Informasi Pribadi) tersimpan di file Excel tak terkontrol, grup WhatsApp, dan bucket cloud lama.

Silo IT-Legal

Legal menulis kebijakan, namun IT tidak memiliki **konfigurasi teknis** untuk menegakkannya.

Realitas Lapangan

Celah Kritis dari Audit 2025

Pemetaan Data Tidak Lengkap

80%

Organisasi tidak dapat melacak siklus hidup penuh dari satu rekaman data pelanggan.

Risiko Pihak Ketiga

Vendor memproses data tanpa **Perjanjian Pemrosesan Data (DPA)** yang diperbarui dan valid.

Defisit Logging

Ketidakmampuan teknis untuk membuktikan **siapa mengakses apa** dan untuk alasan apa.

03 Audit PDP

01 **Audit Pihak Pertama**
Dilakukan oleh unit Auditor Internal untuk memastikan kontrol kepatuhan PDP di Perusahaan

02 **Audit Pihak Kedua**
Dilakukan oleh Auditor Internal atau Eksternal untuk memastikan kontrol kepatuhan PDP di Prosesor risiko tinggi

03 Audit Pihak Ketiga
Dilakukan oleh Auditor Eksternal untuk memastikan impelementasi PDP di Perusahaan sesuai :

- Kontrol Kepatuhan PDP
- Standard ISO 27701
- Kontrol lainnya (misal investigatif dan penghapusan pemusnahan Data Pribadi)

04

04 Asesmen PDP

01 **Asesmen Kesenjangan**
Dilakukan diawal dan diakhir pekerjaan konsultasi PDP untuk mengukur hasil pekerjaan

02 **Asesmen berbasis RoPA**
Dilakukan setelah dokumentasi RoPA untuk menganalisis kesenjangan minimalisasi data, kontraktual, tindakan teknis organisasi, analisis risiko, dsb

03 **Asesmen Kepentingan Sah**
Dilakukan untuk memastikan adanya tujuan, kebutuhan, dan keseimbangan pemrosesan

04 **Asesmen Transfer Data**
Dilakukan untuk memitigasi risiko transfer Data Pribadi ke luar wilayah negara RI

Jebakan Umum

Lima Kesalahan Strategi Fatal

01 **Menganggap PDP sebagai Proyek**

Ini adalah operasional "BAU" (Business As Usual) berkelanjutan, bukan tugas sekali jalan.

02 **Terlalu Mengandalkan ISO 27001**

Keamanan (Kerahasiaan) hanya **30% dari Privasi** (Hak & Tujuan).

03 **Template Overload**

Menggunakan kebijakan generik yang tidak mencerminkan arus data internal aktual.

04 **Mengabaikan DPIA**

Gagal menilai risiko privasi sebelum meluncurkan produk digital baru.

05 **Postur Reaktif**

Menunggu pelanggaran terjadi sebelum menguji rencana Respons Insiden.

Strategi & Roadmap

Strategi 4-Pilar Xynexis

Governance

The "Brain"

Garis pelaporan dan mandat DPO. Struktur pengambilan keputusan strategis.

Process

The "Body"

DPIA, Pemetaan Data, dan Hak Subjek. Eksekusi operasional sehari-hari.

Technology

The "Shield"

Enkripsi, Anonimisasi, dan DLP. Kontrol teknis untuk perlindungan data.

People

The "Soul"

Budaya privasi dan pelatihan spesifik peran. Kesadaran SDM sebagai pertahanan awal.

Pilar 1: Governance (Otak)

Fondasi Organisasi Kepatuhan

Independensi DPO

Memastikan Data Protection Officer melapor langsung ke **Dewan Direksi/Manajemen** untuk menjamin otonomi pengawasan.

Privacy-by-Design

Mengintegrasikan persyaratan privasi dan keamanan ke dalam **SDLC (Software Development Life Cycle)** sejak tahap desain awal.

Pilar 2: Proses & Kontrol

"Kerja Keras" Operasional

RoPA (Record of Processing Activities)

Inventaris pusat dari **seluruh aktivitas pemrosesan data** dalam organisasi. Peta jalan wajib untuk audit.

Kerangka Kerja DPIA

Proses berulang dan terstandarisasi untuk **menilai risiko** dalam setiap inisiatif pemrosesan data berisiko tinggi.

Pilar 3: Teknologi (Perisai)

Enablement Teknologi

Minimisasi Data

Alur kerja otomatis untuk **"Hak untuk Dihapus dan Dimusnahkan"** guna mengurangi footprint data yang tidak perlu.

Kontrol Teknis

Identity & Access Management (IAM) yang dipetakan secara spesifik ke tingkat **sensitivitas Data Pribadi**.

Pilar 4: People

Budaya & Orang

Pelatihan Bertahap

Kesadaran dasar untuk semua karyawan; **"Pelatihan Teknis Mendalam"** khusus untuk IT dan Admin Database.

Latihan Pelanggaran

Menguji kemampuan organisasi secara nyata untuk merespons **simulasi kebocoran data** baik secara teknikal (Cyber Drill) atau prosedural (TTX).

Rencana Aksi

Roadmap Eksekusi 12 Bulan

1

Bulan 1-3

Baseline

Gap Assessment

Data Discovery

2

Bulan 4-6

Foundation

Governance Framework

Legal Alignment

3

Bulan 7-9

Hardening

Technical Controls

Vendor Remediation

4

Bulan 10-12

Validation

External Audit Simulation

Board Reporting

Benchmarking

Model Penilaian Kematangan

Level 1: Ad-Hoc

Tidak ada proses formal. Mode "Pemadam Kebakaran". Reaktif sepenuhnya.

Target 2026

Level 3: Defined

Proses terstandarisasi, didokumentasikan, dan dikomunikasikan. Kepatuhan konsisten.

Level 5: Optimized

Perbaikan berkelanjutan melalui pemantauan otomatis dan analitik prediktif.

Bukti Nyata

Studi Kasus: Institusi Keuangan

Tantangan

Data Terfragmentasi

Data pelanggan tersebar di 5 kantor regional tanpa kontrol pusat. Risiko tinggi kebocoran dan ketidakpatuhan.

14 Hari

Waktu Respons Data

Solusi & Hasil

Sentralisasi & Governance

Implementasi Pemetaan Data Terpusat dan Tata Kelola DPO yang independen.

2 Jam

Waktu Respons Data

Solusi Kami

Portfolio Xynexis: Akselerasi Kesiapan

PDP Readiness Assessment

Analisis kesenjangan (gap analysis) mendetail terhadap persyaratan UU PDP untuk mengidentifikasi risiko kepatuhan.

Managed Privacy Services

Outsource kompleksitas fungsi operasional seperti **DPIA** dan **DPO** kepada ahli kami.

Privacy Tech Integration

Bantuan teknis khusus dalam penerapan teknologi privasi seperti **Enkripsi** & **DLP**.

Fleksibilitas Kerjasama

Model Engagement

Opsi A

The Diagnostic

Scan kematangan terfokus selama 4 minggu untuk identifikasi celah awal.

Opsi B

The Transformation

Eksekusi roadmap end-to-end penuh dari penilaian hingga implementasi kontrol.

Opsi C

Managed Compliance

Dukungan berkelanjutan untuk mempertahankan status "Siap Audit" sepanjang tahun.

Ambil Tindakan

Langkah Pertama

Value Add

Semua peserta mendapatkan akses eksklusif ke "2026 PDP Operational Checklist".

Penawaran Terbatas

5 Pendaftar Pertama menerima Complimentary High-Level External Exposure Scan.

Dialog Strategis

Q&A

Mari Bicara Tentang Realitas Keamanan Anda