

PEMERINTAH KOTA SEMARANG

Peningkatan Kapasitas Perlindungan Data Pribadi dalam Pelayanan Publik

Sesi 1 · Kerangka Hukum PDP bagi Badan Publik

Sesi 2 · Praktik di Pelayanan Publik Kota Semarang

Bimbingan Teknis · Durasi 2 sesi · 2026

Dasar: Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Untuk apa dua sesi ini?

01

Samakan bahasa

ASN memahami data pribadi, pengendali, prosesor, dan dasar sah pemrosesan di badan publik.

02

Hubungkan ke layanan nyata

NIK, KK, bansos, PBB, rekam medis, perizinan, dan pengaduan dipetakan ke kewajiban UU PDP.

03

Tahu batas dan sanksi

Hak warga tidak mutlak menghapus arsip negara, tetapi kebocoran dan penyalahgunaan berkonsekuensi.

04

Siap menindaklanjuti

Notice privasi, minimisasi data, akses internal, retensi, dan notifikasi 3×24 jam menjadi kerja OPD.

Alur materi Sesi 1 dan Sesi 2

SESI 1

Kerangka Hukum PDP bagi Badan Publik

1. Pengertian data pribadi & pemrosesan
2. Subjek, pengendali, prosesor di Pemkot
3. Dasar sah pemrosesan pelayanan publik
4. Hak subjek data dan batasannya
5. Kewajiban pengendali
6. Sanksi administratif & pidana
7. Relasi UU PDP, KIP, Pelayanan Publik
8. CCTV di fasilitas layanan (Pasal 17)

SESI 2

Praktik di Pelayanan Publik Kota Semarang

1. Titik pengumpulan data di lapangan
2. Peta data per OPD unggulan
3. Minimisasi data
4. Berbagi data antar-OPD
5. Notice privasi & hak akses internal
6. Retensi dan pemusnahan
7. Peran Diskominfo, PPID, CSIRT, DPO
8. Lima kasus nyata + cara merespons

SESI 1

Kerangka Hukum PDP bagi Badan Publik

UU No. 27 Tahun 2022 · Pemerintah daerah adalah pengendali data pribadi

Mengapa PDP menjadi urusan setiap OPD?

Badan publik = pengendali

Pemkot menentukan tujuan dan mengendalikan pemrosesan data warga. Bukan hanya urusan Diskominfo.

Layanan = pemrosesan data

Setiap formulir, loket, aplikasi, call center, dan pengaduan adalah pemrosesan data pribadi.

Kepercayaan publik rapuh

Satu file Excel yang bocor atau KK yang beredar di WhatsApp merusak reputasi seluruh Pemkot.

Ada kewajiban + sanksi

Kegagalan perlindungan wajib diberitahukan 3×24 jam. Ada sanksi administratif dan pidana.

Apa itu data pribadi?

Definisi UU 27/2022 Pasal 1

Data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lain, baik langsung maupun tidak langsung, melalui sistem elektronik atau nonelektronik.

Contoh yang sering dilupakan

Nomor HP, email, foto wajah di loket, plat nomor + nama, rekaman CCTV yang bisa mengenali orang, riwayat pengaduan, data penerima bansos.

Bukan hanya NIK dan KK

Selama seseorang bisa dikenali dari data itu—sendiri atau digabung—itu data pribadi. Spreadsheet “anonim” yang masih punya alamat + tanggal lahir tetap berisiko.

Elektronik dan kertas sama

Berkas fisik di loket, fotokopi KK di laci petugas, dan file di Google Drive OPD sama-sama masuk lingkup UU PDP.

Data pribadi umum dan data spesifik

DATA UMUM

Tetap dilindungi, tingkat kehati-hatian standar.

- ▶ Nama lengkap
- ▶ Jenis kelamin
- ▶ Kewarganegaraan
- ▶ Agama
- ▶ Status perkawinan
- ▶ Data lain yang dikombinasikan untuk mengidentifikasi seseorang (NIK, alamat, nomor HP, email)

DATA SPESIFIK

Lebih ketat. Salah kelola = risiko lebih berat.

- ▶ Data dan informasi kesehatan
- ▶ Data biometrik (wajah, sidik jari)
- ▶ Data genetika
- ▶ Catatan kejahatan
- ▶ Data anak
- ▶ Data keuangan pribadi
- ▶ Data lain yang ditetapkan peraturan

Pemrosesan lebih luas dari “menyimpan di server”

Setiap tindakan terhadap data pribadi—dari diambil sampai dihapus—adalah pemrosesan.

01

Perolehan

Formulir loket, aplikasi, fotokopi, wawancara

02

Pengumpulan

Rekap harian, unduhan dari sistem

03

Pengolahan

Verifikasi, scoring bansos, hitung PBB

04

Analisis

Pemetaan penerima, dashboard

05

Penyimpanan

Server, cloud, arsip rak, flashdisk

06

Perbaikan

Update alamat, koreksi NIK

07

Pengumuman

Papan pengumuman, website, media

08

Transfer

Kirim ke OPD lain, bank, vendor

09

Penyebarluasan

Grup WA, email massal, folder bersama

10

Penghapusan

Musnah arsip, hapus akun, retensi habis

Subjek data, pengendali, dan prosesor

SUBJEK DATA

Warga yang datanya diproses

Pemohon KTP, wajib pajak PBB, pasien puskesmas, penerima bansos, pelapor di Lapor Semar, orang tua siswa.

PENGENDALI

Menentukan tujuan & kendali

Pemerintah Kota Semarang / OPD yang memutuskan untuk apa data dikumpulkan dan bagaimana dipakai. Inilah posisi utama Pemkot.

PROSESOR

Memproses atas nama pengendali

Vendor aplikasi, hosting, bank penyalur bansos, pihak ketiga yang mengolah data sesuai perintah OPD—bukan untuk tujuan sendiri.

Satu OPD bisa pengendali untuk layanannya sendiri, sekaligus prosesor jika mengolah data atas perintah OPD lain.

Siapa berperan apa di lingkungan Pemkot Semarang

PIHAK	POSISI UU PDP	CONTOH DI SEMARANG
Wali Kota / Sekda	Pengendali tingkat kota	Menetapkan kebijakan, menanggung akuntabilitas institusi
OPD pemilik layanan	Pengendali operasional	Disdukcapil, Dinsos, Bapenda, Dinkes, DPMPTSP, Disdik, dsb.
Diskominfo	Pengendali + penata kelola TIK	SPBE, aplikasi kota, keamanan informasi, fasilitasi PDP
PPID	Persimpangan KIP dan PDP	Membuka informasi publik tanpa membocorkan data pribadi
Vendor / bank / RS mitra	Prosesor atau pengendali bersama	Tergantung kontrak: siapa menentukan tujuan pemrosesan
Petugas loket & admin	Pelaksana pengendali	Bukan “pemilik data”, tetapi terikat kewajiban yang sama

Enam dasar sah pemrosesan data pribadi

1 Persetujuan sah

Subjek data setuju secara tegas untuk tujuan tertentu.

2 Perjanjian

Diperlukan untuk melaksanakan kontrak dengan subjek data.

3 Kewajiban hukum

Pengendali wajib memproses karena peraturan.

4 Kepentingan vital

Menyelamatkan nyawa subjek data atau orang lain.

5 Tugas publik / kewenangan

Kepentingan umum, pelayanan publik, atau kewenangan peraturan.

6 Kepentingan sah lain

Dengan menimbang keseimbangan hak subjek data.

Dasar sah yang paling sering dipakai Pemkot

Untuk layanan wajib pemerintahan, dasar utamanya biasanya bukan “persetujuan”, melainkan pelaksanaan tugas pelayanan publik atau kewenangan berdasarkan peraturan.

Boleh tanpa persetujuan?

Ya, jika ada dasar hukum yang jelas: Perda, Perwal, UU Administrasi Kependudukan, UU Pajak Daerah, UU Kesehatan, dll.

Tujuan tidak boleh melebar

Data KTP untuk penerbitan dokumen kependudukan tidak otomatis boleh dipakai untuk undangan acara atau dibagikan ke pihak ketiga.

Persetujuan tetap relevan

Untuk data di luar keperluan layanan wajib—misalnya foto kegiatan yang diunggah ke medsos dinas, atau survei nonwajib.

Transparansi tetap wajib

Warga berhak tahu data apa yang diambil, untuk apa, disimpan berapa lama, dan siapa yang mengakses—meski dasar hukumnya bukan consent.

Hak warga atas datanya di tangan Pemkot

01

Informasi

Tahu bahwa datanya diproses, untuk apa, dan oleh siapa.

02

Akses

Meminta salinan atau konfirmasi data yang dikuasai OPD.

03

Perbaikan

Mengoreksi data yang keliru, usang, atau tidak lengkap.

04

Penghapusan

Meminta hapus jika pemrosesan tidak lagi sah—ada batas.

05

Tarik persetujuan

Jika dasar pemrosesan adalah consent, bisa ditarik.

06

Keberatan / batasi

Menolak pemrosesan tertentu yang merugikan haknya.

07

Ganti rugi

Menuntut jika dilanggar dan timbul kerugian.

08

Pengajuan pengaduan

Ke pengendali, lembaga pengawas, atau pengadilan.

Hak penghapusan tidak menghapus arsip negara

Warga berhak meminta penghapusan, tetapi Pemkot tidak boleh menghapus data yang wajib disimpan karena peraturan kearsipan, administrasi kependudukan, perpajakan, kesehatan, atau penegakan hukum.

Boleh / wajib dipertahankan

Register kependudukan, SPPT & riwayat PBB sesuai masa retensi pajak, rekam medis sesuai UU Kesehatan, berkas perizinan yang masih berlaku, bukti pencairan bansos untuk audit, arsip sesuai Jadwal Retensi Arsip.

Patut dihapus / dibatasi

Fotokopi KK di HP petugas setelah layanan selesai, file Excel “siswa rapat” di grup WA, data pendaftar event yang sudah lewat, akun uji coba aplikasi, salinan data di vendor setelah kontrak berakhir.

Empat kewajiban inti yang harus hidup di OPD

1

Tujuan terbatas

Data hanya diproses untuk tujuan yang dinyatakan dan sah. Jangan “sekalian saja” dipakai untuk keperluan lain.

2

Akurasi

Data harus benar, lengkap, dan mutakhir sesuai kebutuhan layanan. Data salah merugikan warga dan instansi.

3

Keamanan

Lindungi kerahasiaan, keutuhan, dan ketersediaan. Termasuk akses orang dalam, bukan hanya peretas.

4

Transparansi

Sampaikan kepada warga data apa yang diambil, dasar hukumnya, dan ke mana mereka bisa bertanya.

Jika data bocor: kewajiban 3×24 jam

BATAS WAKTU

**3 × 24
jam**

Pemberitahuan tertulis kepada subjek data dan lembaga yang berwenang, dihitung sejak pengendali mengetahui kegagalan perlindungan.

Apa yang terungkap

Jenis dan perkiraan lingkup data pribadi yang bocor.

Kapan dan bagaimana

Waktu diketahui serta modus: peretasan, salah unggah, orang dalam, dsb.

Upaya penanganan

Langkah penanggulangan, pemulihan, dan pencegahan berulang.

Jika berdampak luas

Kegagalan yang mengganggu pelayanan publik / kepentingan masyarakat diumumkan kepada publik.

Sanksi administratif dan pidana secara garis besar

ADMINISTRATIF

Untuk pelanggaran kewajiban pengendali/prosesor.

1. Peringatan tertulis
2. Penghentian sementara pemrosesan
3. Penghapusan atau pemusnahan data
4. Ganti rugi
5. Denda administratif — hingga 2% pendapatan tahunan atau sesuai ketentuan pelaksana

PIDANA

Untuk perbuatan yang dilarang, antara lain:

1. Memperoleh atau mengumpulkan data secara melawan hukum
2. Mengungkapkan data pribadi yang bukan miliknya
3. Memalsukan data pribadi
4. Menjual atau membeli data pribadi
5. Ancaman lebih berat jika menyangkut data spesifik atau dilakukan korporasi/pejabat

UU PDP tidak berdiri sendiri

UU 27/2022 PDP

Melindungi data orang.
Membatasi apa yang boleh
diproses, dibagikan, dan
diumumkan.

UU 14/2008 KIP

Mewajibkan keterbukaan
informasi publik. Ada informasi
yang dikecualikan: hak pribadi.

UU 25/2009 Pelayanan Publik

Layanan harus cepat, mudah,
akuntabel—tetap tidak boleh
mengorbankan privasi pemohon.

Perwal Semarang PPID & Pengaduan

Perwal PID/PPID dan Perwal
Pengaduan (termasuk Laporan
Semar) mengatur prosedur lokal.

Cara membacanya di loket dan di PPID

Informasi tentang kinerja dinas, anggaran, dan prosedur layanan = pada prinsipnya publik. Nama, NIK, alamat, nomor HP, riwayat kesehatan, atau status bansos orang tertentu = data pribadi. Uji konsekuensi KIP dan uji tujuan PDP dilakukan sebelum data dikeluarkan.

CCTV dan perekaman di fasilitas pelayanan publik

Pemasangan alat pemroses/pengolah data visual di tempat umum atau fasilitas layanan publik wajib memenuhi syarat.

01 Tujuan terbatas

Keamanan, pencegahan bencana, dan/atau pengaturan lalu lintas atau analisis informasi lalu lintas—bukan untuk memata-matai staf atau warga.

02 Ada pemberitahuan

Pasang papan/stiker yang jelas di area yang terekam. Warga harus tahu bahwa area itu diawasi.

03 Bukan alat identifikasi bebas

Rekaman tidak dipakai untuk mengidentifikasi seseorang kecuali sesuai ketentuan peraturan.

04 Akses dan retensi

Siapa boleh menonton, berapa lama disimpan, dan kapan dihapus harus diatur SOP. Jangan disimpan di HP pribadi petugas.

SESI 2

Praktik di Pelayanan Publik Kota Semarang

Dari loket, aplikasi, dan pengaduan sampai lima kasus yang sering terjadi

Di mana data warga mulai masuk ke Pemkot?

01

Loket & MPP

Formulir kertas, fotokopi KK/KTP, antrian, percakapan yang dicatat petugas.

02

Aplikasi layanan

e-PBB, e-BPHTB, perizinan, pendaftaran daring, unggah dokumen.

03

Call center / WA dinas

Warga mengirim foto KTP ke nomor petugas. Sering tanpa kendali retensi.

04

Pengaduan

Lapor Semar, SP4N-LAPOR!, tatap muka. Identitas pelapor wajib dijaga.

05

Survei & event

Daftar hadir, doorprize, foto kegiatan, link Google Form.

06

Integrasi antar-OPD

API, file sharing, permintaan data “untuk rapat pimpinan”.

Contoh OPD dan jenis data yang dikelola

OPD	DATA TYPICAL	TINGKAT HATI-HATI
Disdukcapil	NIK, KK, akta, foto, alamat, status keluarga	Data umum + data anak
Dinsos	NIK, kondisi sosial ekonomi, rekening, anggota rumah tangga	Data umum + keuangan
Bapenda	NOP, NJOP, identitas wajib pajak, transaksi BPHTB	Data umum + keuangan
Dinkes / puskesmas	Rekam medis, diagnosis, imunisasi, lab	Data spesifik kesehatan
DPMPTSP / perizinan	NIK, NPWP, alamat usaha, dokumen pendirian	Data umum + keuangan
PPID / Diskominfo	Permohonan informasi, log akses, data pengaduan	Campuran; uji konsekuensi

Minimisasi data: jangan minta yang tidak perlu

Setiap kolom formulir harus bisa dijawab: “Untuk langkah layanan yang mana data ini wajib ada?” Jika tidak wajib, hapus dari formulir.

HINDARI

- Meminta NPWP untuk layanan yang tidak terkait pajak.
- Meminta fotokopi KK lengkap padahal cukup NIK pemohon.
- Menyimpan foto KTP di HP petugas “jaga-jaga”.
- Mengisi kolom agama/pekerjaan tanpa keperluan layanan.

LAKUKAN

- Rancang formulir ulang per jenis layanan.
- Masking NIK di antrian dan papan pengumuman.
- Pakai data yang sudah ada di sistem, jangan minta ulang.
- Hapus salinan setelah verifikasi jika arsip resmi sudah ada.

Kapan data boleh dibagikan ke OPD lain?

01

Ada dasar hukum

Peraturan memerintahkan atau mengizinkan berbagi untuk tujuan tertentu (mis. verifikasi bansos, penegakan pajak).

02

Tujuan sama atau kompatibel

Tidak “numpang” data kependudukan untuk keperluan di luar layanan yang sah.

03

Data seminimal mungkin

Kirim kolom yang diperlukan saja, bukan dump database.

04

Ada jejak dan penanggung jawab

Surat/permohonan resmi, log akses, PIC, dan jangka waktu akses.

05

Keamanan saluran

Bukan WhatsApp pribadi. Gunakan kanal resmi, enkripsi, atau ruang data terbatas.

06

Vendor ikut aturan pengendali

Perjanjian memuat tujuan, larangan pakai ulang, penghapusan, dan audit.

Notice privasi dan hak akses internal

NOTICE PRIVASI

Wajib ada di loket, website, dan aplikasi.

- Identitas pengendali (OPD / Pemkot)
- Dasar hukum dan tujuan pemrosesan
- Jenis data yang dikumpulkan
- Pihak yang mungkin menerima data
- Lama penyimpanan secara umum
- Cara subjek data mengajukan hak
- Kontak pengaduan / PPID / Diskominfo

HAK AKSES INTERNAL

Jabatan tidak otomatis membuka semua data.

- NIK/KK: petugas berwenang + log
- Data kesehatan: tenaga kesehatan
- Data bansos: petugas verifikasi
- Data pajak: petugas perpajakan
- Pimpinan: ringkasan, bukan dump mentah
- Magang / honorer: akses minimal
- Password bersama = pelanggaran budaya

Retensi dan pemusnahan

1

Kumpulkan

Hanya data yang perlu untuk layanan saat ini.

2

Gunakan

Sesuai tujuan. Catat siapa mengakses.

3

Simpan

Ikuti Jadwal Retensi Arsip + aturan sektor.

4

Tinjau

Data mati / duplikat / sisa proyek dipilah.

5

Musnahkan

Digital dan kertas. Buat BA pemusnahan.

Praktik yang sering terlewat

Flashdisk dinas, grup WhatsApp “Arsip 2023”, folder Google Drive yang masih dibuka untuk vendor lama, dan mesin fotokopi yang menyimpan scan. Pemusnahan kertas tanpa merusak keterbacaan NIK bukan pemusnahan. Setelah kontrak vendor selesai, minta konfirmasi tertulis bahwa data telah dihapus.

Siapa mengerjakan apa setelah pelatihan ini?

Diskominfo

Standar SPBE, keamanan sistem, notice privasi digital, pendampingan OPD, kanal insiden siber.

PPID

Uji konsekuensi KIP vs PDP, menolak/melepas informasi dengan dasar, jaga identitas pemohon.

CSIRT / persandian

Deteksi dan respons insiden, harden sistem, pendampingan teknis saat dugaan peretasan.

Bagian Hukum

Dasar wewenang berbagi data, klausul kontrak vendor, telaah Perwal/SOP PDP.

OPD pemilik layanan

Bersihkan formulir, atur akses staf, latih loket, laporkan insiden, tunjuk PIC data.

Pejabat / pengelola PDP

Fungsi DPO: nasihat, pengawasan internal, titik kontak subjek data dan pengawas.

Kebiasaan kecil yang sudah termasuk pemrosesan

Kasus 1 · Petugas loket memotret KK lalu membagikannya di grup WhatsApp internal

Masalah: HP pribadi, grup tidak terkontrol, anggota bisa keluar-masuk, tidak ada retensi. Itu penyebaran data pribadi.

Respons: hentikan praktik, hapus unggahan, ganti ke kanal resmi / SISFO, buat aturan “dilarang foto dokumen warga ke HP pribadi”, tegur dan dokumentasikan.

Kasus 2 · File Excel penerima bansos terunggah ke folder yang bisa diakses umum

Masalah: kegagalan perlindungan. Data sosial-ekonomi + NIK beredar.

Respons: tarik tautan, ubah hak akses, cek log unduhan, nilai dampak, siapkan notifikasi 3×24 jam, laporkan ke Diskominfo/CSIRT, beritahu pimpinan, evaluasi mengapa file diletakkan di folder publik.

Aplikasi layanan diretas — clock 3×24 jam mulai berjalan

Jam ke-0–3

Isolasi sistem, jangan panik-format bukti. Hubungi CSIRT/Diskominfo, vendor, pimpinan OPD.

Jam ke-3–12

Pastikan lingkup: data apa, berapa record, apakah masih diakses penyerang. Amankan log.

Jam ke-12–24

Susun draf pemberitahuan: jenis data, waktu, modus, langkah pemulihan, kontak pengaduan.

Maks. 3×24 jam

Kirim pemberitahuan tertulis ke subjek data (secara proporsional) dan lembaga berwenang. Jika mengganggu layanan publik, siapkan pengumuman publik.

Keterbukaan informasi dan vendor

Kasus 4 · Permohonan informasi publik memuat data pribadi pihak ketiga

Contoh: daftar lengkap penerima bansos beserta NIK dan alamat, atau salinan pengaduan yang menyingkap identitas terlapor.

Respons PPID: uji konsekuensi. Beri data agregat atau data yang sudah dianonimkan. Identitas pelapor Laporan Semar dijaga. Jika ragu, konsultasikan Hukum + Diskominfo sebelum melepas.

Kasus 5 · Vendor aplikasi daerah menyimpan data di luar kendali OPD

Masalah: pengendali tetap Pemkot. Prosesor tidak boleh punya tujuan sendiri, menyalin ke cloud pribadi, atau menolak mengembalikan data.

Respons: audit kontrak, klausul PDP, lokasi data, hak audit, kewajiban hapus saat kontrak selesai, larangan subprosesor tanpa izin, dan denda jika bocor karena kelalaian vendor.

Tujuh langkah yang bisa dimulai minggu ini

- | | | |
|----|--------------------------------------|---|
| 01 | Tunjuk PIC PDP di OPD | Satu orang yang jadi titik kontak insiden dan pertanyaan warga. |
| 02 | Audit formulir & aplikasi | Coret kolom yang tidak wajib untuk layanan. |
| 03 | Pasang notice privasi | Loket, website, dan layar aplikasi. Bahasa singkat. |
| 04 | Kunci akses internal | Hapus akun bersama. Aktifkan log. Cabut akses yang pindah tugas. |
| 05 | Bersihkan kanal liar | Grup WA berisi scan KK, Drive publik, flashdisk liar. |
| 06 | Cek kontrak vendor | Klausul tujuan, hapus data, larangan pakai ulang, notifikasi insiden. |
| 07 | Siapkan SOP 3×24 jam | Nomor yang dihubungi, template pemberitahuan, alur ke Diskominfo. |

PESAN KUNCI

Pelayanan publik yang cepat tetap wajib melindungi data warga.

Pemkot Semarang adalah pengendali. Setiap OPD, petugas loket, admin aplikasi, dan vendor ikut menanggung kewajiban itu. Diskusi dan tanya jawab dibuka.

Pemerintah Kota Semarang · 2026
UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi