



PEMERINTAH PROVINSI JAWA TENGAH
DINAS KOMUNIKASI, INFORMATIKA, DAN DIGITAL

KEPUTUSAN KEPALA DINAS KOMUNIKASI, INFORMATIKA, DAN DIGITAL
PROVINSI JAWA TENGAH

NOMOR : 500.12.10/2 TAHUN 2026

TENTANG

PEDOMAN PELINDUNGAN DATA PRIBADI
DI LINGKUNGAN DINAS KOMUNIKASI, INFORMATIKA, DAN DIGITAL

KEPALA DINAS KOMUNIKASI, INFORMATIKA, DAN DIGITAL
PROVINSI JAWA TENGAH,

- Menimbang : a. bahwa dalam rangka memastikan pemrosesan Data Pribadi di lingkungan Dinas Komunikasi, Informatika, dan Digital Provinsi Jawa Tengah diselenggarakan secara aman dan bertanggung jawab, perlu dirumuskan suatu pedoman perlindungan data pribadi di lingkungan Dinas Komunikasi, Informatika, dan Digital Provinsi Jawa Tengah;
- b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu ditetapkan Keputusan Kepala Dinas Komunikasi, Informatika, dan Digital Provinsi Jawa Tengah tentang Pedoman Pelindungan Data Pribadi di Lingkungan Dinas Komunikasi, Informatika, dan Digital Provinsi Jawa Tengah.
- Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58,

- Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubahh terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);
2. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
 3. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820);
 4. Undang-Undang Nomor 11 Tahun 2023 tentang Provinsi Jawa Tengah (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 6867);
 5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
 6. Peraturan Gubernur Nomor 2 Tahun 2026 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Dinas dan Badan (Berita Daerah Provinsi Jawa Tengah Tahun 2026 Nomor 2).

MEMUTUSKAN :

- Menetapkan :
KESATU : Pedoman Pelindungan Data Pribadi di Lingkungan Dinas Komunikasi, Informatika, dan Digital Provinsi Jawa Tengah sebagaimana tercantum dalam Lampiran

- yang merupakan bagian tidak terpisahkan dari Keputusan Kepala Dinas ini.
- KEDUA : Pedoman Pelindungan Data Pribadi sebagaimana dimaksud dalam Diktum KESATU berisi Ketentuan Umum Pelindungan Data Pribadi.
- KETIGA : Pedoman Pelindungan Data Pribadi sebagaimana disebut dalam Diktum KESATU dilaksanakan sesuai tugas, fungsi, dan tanggung jawab masing-masing unit kerja di lingkungan Dinas Komunikasi, Informatika, dan Digital Provinsi Jawa Tengah.
- KEEMPAT : Panduan teknis pelaksanaan Pedoman Pelindungan Data Pribadi sebagaimana dimaksud dalam Diktum KETIGA ditetapkan oleh Kepala Dinas.
- KELIMA : Biaya yang timbul sebagai akibat dari pelaksanaan Keputusan Kepala Dinas ini, dibebankan kepada DPA Dinas Komunikasi, Informatika, dan Digital serta sumber lain yang sah dan tidak mengikat berdasarkan ketentuan peraturan perundang-undangan.
- KEENAM : Keputusan Kepala Dinas ini mulai berlaku pada tanggal ditetapkan

Ditetapkan di : Semarang
Pada tanggal : 1 Agustus 2026

KEPALA DINAS KOMUNIKASI, INFORMATIKA, DAN DIGITAL
PROVINSI JAWA TENGAH



LILIK HENRY RISTANTO

SALINAN keputusan ini disampaikan kepada Yth:

1. Gubernur Provinsi Jawa Tengah;
2. Wakil Gubernur Provinsi Jawa Tengah;
3. Sekretaris Daerah Provinsi Jawa Tengah;
4. Asisten Administrasi Sekretaris Daerah Provinsi Jawa Tengah; dan
5. Arsip

LAMPIRAN KEPUTUSAN KEPALA DINAS
KOMUNIKASI, INFORMATIKA, DAN DIGITAL
PROVINSI JAWA TENGAH NOMOR
500.12.10/2 TAHUN 2026 TENTANG PEDOMAN
PELINDUNGAN DATA PRIBADI DI
LINGKUNGAN DINAS KOMUNIKASI,
INFORMATIKA, DAN DIGITAL

KETENTUAN UMUM PELINDUNGAN DATA PRIBADI
DI LINGKUNGAN DINAS KOMUNIKASI, INFORMATIKA, DAN DIGITAL
PROVINSI JAWA TENGAH

A. Pendahuluan

Pemrosesan Data Pribadi merupakan aspek yang sangat penting dalam penyelenggaraan layanan publik di lingkungan Dinas Komunikasi, Informatika, dan Digital (Diskomdigi). Dalam setiap interaksi antara masyarakat dengan pemerintah melalui layanan digital, aplikasi, portal informasi, maupun layanan manual terdapat proses pengumpulan, pencatatan, pengolahan, penyimpanan, penggunaan, dan penghapusan Data Pribadi yang harus dilakukan sesuai dengan ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Pada konsep Pelindungan Data Pribadi aspek privasi data dan keamanan data menjadi prasyarat utama untuk menjaga kepercayaan masyarakat serta untuk memastikan bahwa layanan publik berjalan secara efektif dan akuntabel.

Transformasi digital menuju Pemerintah Digital (PEMDI) menuntut adanya tata kelola Pelindungan Data Pribadi yang selaras dengan prinsip Pelindungan Data Pribadi sebagaimana amanat UU PDP. Dalam ekosistem yang digital yang semakin kompleks, risiko kebocoran data, akses tidak sah, dan penyalahgunaan Data Pribadi menjadi tantangan yang harus diantisipasi melalui kebijakan, prosedur, dan mekanisme pelindungan yang memadai. Oleh karena itu, Pelindungan Data Pribadi bukan hanya kewajiban hukum, namun juga fondasi utama dalam membangun layanan publik digital yang aman, terpercaya, dan berorientasi pada kepentingan masyarakat.

Diskomdigi sebagai instansi yang mengelola berbagai layanan publik berbasis teknologi informasi memiliki peran strategis dalam memastikan bahwa seluruh pemrosesan Data Pribadi dilakukan sesuai prinsip Pelindungan Data Pribadi. Penerapan prinsip tersebut menjadi bagian integral dari upaya Dinas dalam memperkuat tata kelola pemerintahan yang modern dan responsif terhadap perkembangan teknologi dan isu terkini.

Pedoman ini disusun sebagai landasan bagi seluruh unit kerja di lingkungan Diskomdigi dalam melaksanakan Pelindungan Data Pribadi secara konsisten dan terstruktur. Dokumen ini menjadi instrumen penting dalam mendukung percepatan transformasi digital di Provinsi Jawa Tengah, dengan memastikan bahwa setiap layanan publik yang dikelola oleh Diskomdigi menerapkan standar Pelindungan Data Pribadi yang memadai, sehingga tercipta ekosistem layanan digital yang aman, terpercaya, dan berpihak pada kepentingan masyarakat.

B. Ketentuan Umum

1. Data Pribadi adalah 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.
2. Pelindungan Data Pribadi adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional Subjek Data Pribadi.
3. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.
4. Pengendali Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau

bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi.

5. Unit Pengendali Data Pribadi adalah unit kerja di Dinas Komunikasi, Informatika, dan Digital Provinsi Jawa Tengah yang melakukan pemrosesan Data Pribadi sesuai dengan tugas dan fungsinya.
6. Prosesor Data Pribadi adalah pihak yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan Data Pribadi atas nama Pengendali Data Pribadi.
7. Pejabat atau Petugas Pelindung Data Pribadi adalah pejabat atau pegawai yang ditunjuk untuk mengawasi kepatuhan Pelindungan Data Pribadi.
8. Subjek Data Pribadi adalah orang perseorangan yang pada dirinya melekat data pribadi atau yang datanya diproses, baik secara elektronik maupun nonelektronik.
9. Dinas Komunikasi, Informatika, dan Digital Provinsi Jawa Tengah yang selanjutnya disebut Diskomdigi adalah perangkat daerah yang menyelenggarakan urusan komunikasi dan informatika, urusan persandian, dan urusan statistik.
10. Kepala Dinas adalah kepala perangkat daerah yang menangani urusan komunikasi dan informatika, urusan persandian, dan urusan statistik.

C. Maksud dan Tujuan

Pedoman ini dimaksudkan sebagai landasan perumusan dan pelaksanaan Pelindungan Data Pribadi di lingkungan Diskomdigi. Tujuan pedoman ini adalah:

1. Menjamin pemenuhan prinsip Pelindungan Data Pribadi dalam seluruh aktivitas pemrosesan Data Pribadi di lingkungan Diskomdigi.
2. Memberikan kepastian hukum, tata kelola, dan standar operasional yang terukur bagi unit kerja dalam pemrosesan data pribadi, termasuk dalam penyusunan standar operasional prosedur, pembagian peran, pengendalian risiko, dan pengawasan internal.

3. Mendorong koordinasi dan sinergi antar unit kerja di lingkungan Diskomdigi dalam mendukung transformasi digital.

D. Ruang Lingkup

Ruang Lingkup Pedoman ini meliputi:

1. Organisasi; dan
2. Program Pelindungan Data Pribadi.

E. Ketentuan Pelindungan Data Pribadi

1. Kebijakan Umum

Diskomdigi selaku Pengendali Data Pribadi melaksanakan kebijakan umum Pelindungan Data Pribadi sesuai dengan ketentuan dalam UU PDP meliputi kewajiban untuk:

- a. menerapkan prinsip Pelindungan Data Pribadi;
- b. melakukan pemrosesan Data Pribadi sesuai dengan tujuan pemrosesan;
- c. menyusun dan menyediakan dasar pemrosesan Data Pribadi yang relevan dalam setiap aktivitas pemrosesan Data Pribadi;
- d. memfasilitasi pemenuhan hak Subjek Data Pribadi;
- e. menyampaikan informasi pemrosesan Data Pribadi sesuai dengan tujuan pemrosesan Data Pribadi dan peraturan perundang-undangan;
- f. menjamin integritas Data Pribadi dengan memastikan akurasi, kelengkapan, dan konsistensi setiap Data Pribadi yang diproses;
- g. memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi, termasuk memberikan penolakan permohonan perubahan Data Pribadi sesuai peraturan perundang-undangan;
- h. melakukan perekaman seluruh kegiatan pemrosesan Data Pribadi;
- i. memberikan akses kepada Subjek Data Pribadi terhadap Data Pribadinya dan rekam jejak pemrosesan Data Pribadi;

- j. melakukan penilaian dampak Pelindungan Data Pribadi dalam hal melaksanakan pemrosesan Data Pribadi yang memiliki potensi risiko tinggi;
- k. menyusun dan menerapkan langkah teknis operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan;
- l. menentukan tingkat keamanan Data Pribadi;
- m. menjaga kerahasiaan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;
- n. melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan Data Pribadi;
- o. melindungi Data Pribadi dari pemrosesan yang tidak sah;
- p. mencegah Data Pribadi diakses secara tidak sah dengan menerapkan sistem keamanan terhadap Data Pribadi yang diproses dan/atau memproses Data Pribadi menggunakan sistem elektronik yang andal, aman, dan bertanggung jawab;
- q. menghentikan pemrosesan Data Pribadi dalam hal terdapat penarikan kembali persetujuan;
- r. menunda dan membatasi pemrosesan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;
- s. mengakhiri pemrosesan Data Pribadi sesuai ketentuan peraturan perundang-undangan;
- t. menghapus atau memusnahkan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan, termasuk menetapkan kebijakan retensi Data Pribadi;
- u. menunjuk Pejabat atau Petugas Pelindungan Data Pribadi;
- v. merencanakan aktivitas pemrosesan Data Pribadi dari atau ke luar wilayah hukum Negara Republik Indonesia, termasuk mematuhi kriteria transfer Data Pribadi ke luar wilayah hukum Negara Kesatuan Republik Indonesia;
- w. menyampaikan pemberitahuan kegagalan Pelindungan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan; dan

- x. melaksanakan perintah lembaga di bidang Pelindungan Data Pribadi dalam rangka penyelenggaraan Pelindungan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan.

2. Organisasi

Pedoman Pelindungan Data Pribadi dilaksanakan oleh unit kerja di lingkungan Diskomdigi yang terdiri sebagai berikut:

a. Pengendali Data Pribadi

- 1) Diskomdigi merupakan Pengendali Data Pribadi yang menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi di lingkungan Diskomdigi sesuai dengan ketentuan UU PDP.
- 2) Diskomdigi selaku Pengendali Data Pribadi direpresentasikan oleh Kepala Dinas sebagai kesatuan unsur pimpinan di Diskomdigi.
- 3) pengendalian Data Pribadi di Diskomdigi dilaksanakan berkaitan dengan penyelenggaraan pemerintahan daerah terkait dengan urusan komunikasi dan informatika, urusan persandian, urusan statistik, dan pelaksanaan fungsi lain yang diberikan oleh kepala daerah.

b. Unit Pengendali Data Pribadi

- 1) pengendalian Data Pribadi terdiri dari aktivitas atau beberapa aktivitas pemrosesan Data Pribadi yang dilaksanakan oleh Pengendali Data Pribadi.
- 2) Unit Pengendali Data Pribadi di lingkungan Diskomdigi dilaksanakan oleh unit kerja di lingkungan Diskomdigi, termasuk sumber daya manusia yang terlibat di dalam unit kerja.
- 3) Secara umum, peran unit kerja selaku Unit Pengendali Data Pribadi yaitu melaksanakan pelaksanaan aktivitas pemrosesan Data Pribadi di lingkungan Diskomdigi berkaitan dengan penyelenggaraan tugas dan fungsi dari masing-masing unit kerja sesuai dengan urusan konkuren masing-masing.

c. Prosesor Data Pribadi

- 1) Pengendali Data Pribadi, melalui Unit Pengendali Data Pribadi dapat menunjuk Prosesor Data Pribadi untuk melaksanakan aktivitas atau beberapa aktivitas pemrosesan Data Pribadi di lingkungan Diskomdigi untuk dan atas nama Pengendali Data Pribadi berkaitan dengan aktivitas penyelenggaraan tugas dan fungsi dari masing-masing unit kerja sesuai dengan urusan konkuren masing-masing.
 - 2) Prosesor Data Pribadi dapat meliputi orang perseorangan, badan publik, atau organisasi internasional.
 - 3) Setiap pimpinan unit kerja bertanggung jawab memimpin, mengoordinasikan dan memberikan pengarahan serta petunjuk untuk melakukan pengawasan terhadap setiap Prosesor Data Pribadi dalam pemrosesan Data Pribadi di bawah kendalinya serta melaporkannya secara berkala kepada Pengendali Data Pribadi.
 - 4) Prosesor Data Pribadi dimaksud termasuk:
 - a) penyedia barang/jasa pemerintah;
 - b) subkontraktor;
 - c) mitra Diskomdigi dalam negeri atau luar negeri; atau
 - d) pihak lain yang memiliki perikatan dengan Diskomdigi.
 - 5) Dalam suatu kewajiban kontraktual untuk melindungi Data Pribadi, Prosesor Data Pribadi wajib mematuhi standar keamanan setara (misalnya tersertifikasi SNI ISO/IEC 27001).
 - 6) Unit Pengendali Data Pribadi yang berkaitan dengan penyelenggaraan pengadaan barang dan jasa pemerintah di lingkungan Diskomdigi membuat panduan Pelindungan Data Pribadi berkaitan dengan aspek kontraktual dengan pihak ketiga yang berkontrak dengan Diskomdigi.
- d. Pejabat atau Petugas Pelindungan Data Pribadi
- 1) Pejabat atau Petugas Pelindung Data Pribadi ditetapkan oleh Pengendali Data Pribadi yang berjumlah paling sedikit 1 (satu) orang yang dapat berasal dari dalam atau luar Diskomdigi.

- 2) Penetapan Pejabat atau Petugas Pelindung Data Pribadi didasarkan pada aspek profesionalitas, pengetahuan mengenai hukum, praktik Pelindungan Data Pribadi, dan kemampuan untuk memenuhi tugas-tugasnya.
- 3) Pejabat atau Petugas Pelindung Data Pribadi memiliki tugas, meliputi:
 - a) menginformasikan dan memberikan saran kepada Pengendali Data Pribadi agar mematuhi ketentuan peraturan perundang-undang terkait Pelindungan Data Pribadi;
 - b) memantau dan memastikan kepatuhan Pengendali Data Pribadi lainnya dengan pedoman dan peraturan perundang-undangan terkait Pelindungan Data Pribadi;
 - c) memantau dan memastikan kepatuhan unit kerja terhadap pedoman dan peraturan perundang-undangan terkait Pelindungan Data Pribadi;
 - d) memberikan saran kepada Pengendali Data Pribadi dan unit kerja mengenai penilaian dampak Pelindungan Data Pribadi dan penilaian lainnya;
 - e) berkoordinasi dan bertindak sebagai narahubung untuk isu berkaitan dengan pemrosesan Data Pribadi;
 - f) memanggil Unit Pengendali Data Pribadi atau pihak lain untuk dimintai keterangan berkaitan dengan aktivitas pemrosesan Data Pribadi di lingkungan Diskomdigi;
 - g) beroperasi secara objektif dan tidak diberhentikan atau dihukum karena menjalankan tugasnya sesuai dengan ketentuan peraturan perundang-undangan;
 - h) mendapatkan dukungan teknis dan administratif; dan
 - i) mendapatkan akses pada aktivitas pemrosesan di lingkungan Diskomdigi.

e. Pihak Lain

- 1) Pengendali Data Pribadi, melalui Unit Pengendali Data Pribadi, dapat melibatkan pihak lain yang terlibat atau terkait dalam aktivitas pemrosesan Data Pribadi.

- 2) Pihak lain dapat berupa orang perseorangan, badan publik, atau organisasi internasional yang bekerja untuk dan atas nama Diskomdigi namun sejak awal tidak spesifik diperintahkan untuk memproses Data Pribadi meski pekerjaannya berhubungan secara langsung atau tidak langsung dengan pemrosesan Data Pribadi berdasarkan suatu perintah kerja atau perjanjian kerja sama.
- 3) Setiap pimpinan unit kerja bertanggung jawab memimpin, mengoordinasikan, dan memberikan pengarahan serta petunjuk untuk melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan Data Pribadi di bawah kendalinya serta melaporkannya secara berkala kepada Kepala Dinas.

f. Koordinator Teknis

Ketua Kelompok Kerja pada Bidang Persandian dan Keamanan Siber bertindak selaku Koordinator Teknis Pelindungan Data Pribadi di lingkungan Diskomdigi, termasuk menjalankan fungsi fasilitasi, konsultasi, dan koordinasi antar unit kerja, instansi pemerintah, dan pihak lain sehubungan dengan implementasi Pelindungan Data Pribadi.

3. Program Pelindungan Data Pribadi

Program Pelindungan Data Pribadi dilaksanakan oleh unit kerja di lingkungan Diskomdigi yang berkedudukan sebagai Unit Pengendali Data Pribadi dengan melaksanakan program, antara lain:

a. Pengidentifikasian

- 1) Unit kerja melakukan pengidentifikasian Data Pribadi dalam lingkup pemrosesan Data Pribadi.
- 2) Sasaran identifikasi dimaksud meliputi dokumen, teknologi, sistem informasi, atau pihak-pihak yang terlibat dalam aktivitas pemrosesan Data Pribadi.
- 3) Pengidentifikasian dimaksud dilakukan pada setiap tahapan aktivitas atau siklus pemrosesan Data Pribadi sesuai dengan tugas dan fungsi unit kerja.

- 4) Proses identifikasi ditindaklanjuti dengan inventarisasi, klasifikasi, dan penilaian dampak risiko pemrosesan Data Pribadi, termasuk melakukan perekaman aktivitas pemrosesan Data Pribadi di lingkup Unit Kerja.
- b. Penentuan tujuan pemrosesan Data Pribadi yang relevan
- 1) Unit kerja wajib memastikan dalam pelaksanaan siklus pemrosesan Data Pribadi dilaksanakan sesuai dengan tujuan pemrosesan Data Pribadi yang telah ditetapkan.
 - 2) Unit kerja dalam menentukan tujuan pemrosesan Data Pribadi dapat merujuk pada tugas dan fungsi unit kerja yang ditetapkan oleh peraturan perundang-undangan atau kebijakan unit organisasi yang ditetapkan di awal pemrosesan.
 - 3) Unit kerja wajib menyampaikan pemberitahuan tujuan pemrosesan Data Pribadi kepada Subjek Data Pribadi.
- c. Penyediaan dasar pemrosesan Data Pribadi yang relevan
- Pemrosesan Data Pribadi wajib berdasarkan suatu dasar pemrosesan, yang terdiri dari:
- 1) 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;
 - 2) pemenuhan kewajiban perjanjian dalam hal Subjek Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Subjek Data Pribadi pada saat akan melakukan perjanjian;
 - 3) pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;
 - 4) pemenuhan perlindungan kepentingan vital Subjek Data Pribadi;
 - 5) pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengendali Data Pribadi berdasarkan ketentuan peraturan perundang-undangan; dan/atau

- 6) pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan Pengendali Data Pribadi dan hak Subjek Data Pribadi.

Khusus untuk anak-anak atau penyandang disabilitas, persetujuan orang tua atau wali dilaksanakan sesuai dengan regulasi yang berlaku.

d. Siklus hidup pemrosesan Data Pribadi

Unit kerja melakukan pemrosesan Data Pribadi sesuai lingkup tugas dan fungsi, meliputi siklus hidup berupa:

1) Pemerolehan dan Pengumpulan

- a) Dalam hal pemerolehan dan pengumpulan Data Pribadi, unit kerja wajib memastikan proses identifikasi, kesesuaian dengan tujuan pemrosesan, serta memiliki dasar pemrosesan yang relevan.
- b) Informasi terkait pemrosesan Data Pribadi tersebut harus disampaikan kepada Subjek Data Pribadi dengan cara sederhana, berbahasa Indonesia, mudah diakses, dan memastikan tersedianya bukti persetujuan Subjek Data Pribadi.
- c) Proses perolehan dan pengumpulan dimaksud dilakukan melalui saluran yang aman untuk melindungi Data Pribadi selama proses pengiriman (*data in-transit*) dan bahwa data yang diterima dicatat serta ditangani sesuai tingkat kerahasiaannya.

2) Pengolahan dan Penganalisisan

- a) Pengolahan dan penganalisisan Data Pribadi dilakukan setelah memastikan kesesuaian tujuan dan dasar pemrosesan Data Pribadi.
- b) Informasi metode dan rencana pengolahan wajib disampaikan kepada Subjek Data Pribadi.
- c) Jika pengolahan menggunakan teknologi otomatis seperti pemprofilan yang dapat berdampak hukum atau

signifikan pada Subjek Data Pribadi, maka unit kerja harus memberikan penjelasan yang memadai, memfasilitasi hak keberatan, dan menyediakan alternatif pemrosesan lain jika keberatan Subjek Data Pribadi dimaksud beralasan untuk dikabulkan.

- d) Setiap pengolahan tambahan di luar tujuan awal harus diinformasikan kepada Subjek Data Pribadi secara terpisah.
- e) Selama proses pengolahan berlangsung, unit kerja wajib menjaga keamanan data dengan membatasi akses serta melindungi data agar tidak disalahgunakan atau diakses tanpa izin.

3) Penyimpanan

- a) Penyimpanan Data Pribadi dilakukan dengan memperhatikan kerahasiaan, integritas, dan ketersediaan sesuai ketentuan keamanan pemrosesan Data Pribadi.
- b) Unit kerja wajib menetapkan aturan pembatasan hak akses, pencatatan riwayat akses, serta memastikan bahwa Data Pribadi yang disimpan terlindungi dari perubahan atau penyalahgunaan.
- c) Untuk menjaga kerahasiaan, unit kerja harus menerapkan langkah pengamanan yang memadai terhadap Data Pribadi yang tersimpan (*data at-rest*), paling sedikit dengan menerapkan enkripsi sesuai dengan klasifikasi informasi dan melaksanakan audit secara berkala.
- d) Integritas Data Pribadi dijaga melalui pemeriksaan keakuratan dan pencatatan setiap perubahan.
- e) Ketersediaan Data Pribadi dipastikan melalui langkah pemulihan apabila terjadi insiden, termasuk pencadangan data secara berkala.
- f) Sesuai ketentuan peraturan terkait dengan sistem pemerintahan berbasis elektronik, penyimpanan Data

Pribadi harus dilakukan pada pusat data yang berlokasi di wilayah Indonesia.

4) Perbaikan dan Pembaruan

- a) Dalam rangka memastikan kebenaran, kelengkapan, dan konsisten Data Pribadi, unit kerja wajib melakukan verifikasi melalui pencocokan Data Pribadi, klarifikasi kepada Subjek Data Pribadi, serta penilaian atas permintaan pembaruan atau perbaikan.
- b) Dalam hal ditemukan ketidakakuratan atau ketidakonsistenan, pemrosesan Data Pribadi ditunda hingga perbaikan dilakukan.
- c) Setiap perubahan, pelengkapan, atau koreksi didokumentasikan dan hasilnya diberitahukan kepada Subjek Data Pribadi.
- d) Unit kerja wajib menjaga keamanan data, termasuk perlindungan ketika data sedang diakses atau digunakan (*data in-use*).
- e) Pemberitahuan juga dilakukan jika ada pemutakhiran Data Pribadi beserta alasan pemutakhiran.
- f) Unit kerja wajib menolak memberikan akses perubahan terhadap Data Pribadi kepada Subjek Data Pribadi dalam hal membahayakan keamanan, kesehatan fisik, atau kesehatan mental Subjek Data Pribadi dan/atau orang lain, berdampak pada pengungkapan Data Pribadi milik orang lain; dan/atau bertentangan dengan kepentingan pertahanan dan keamanan nasional.

5) Penampilan, Pengumuman, Transfer, Penyebarluasan, atau Pengungkapan

- a) Penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan Data Pribadi dapat dilakukan untuk tujuan tertentu, baik di internal Diskomdigi atau di luar Diskomdigi.
- b) Aktivitas ini harus didasarkan pada suatu dasar pemrosesan, dan mekanismenya dilakukan dengan pengamanan tambahan yang memadai seperti enkripsi

dan dilengkapi dokumentasi seperti berita acara serah terima data.

- c) Khusus terhadap transfer ke luar negeri, Diskomdigi harus memastikan negara tempat di mana Data Pribadi ditransfer memiliki Pelindungan Data Pribadi harus setara atau lebih tinggi dari UU PDP Indonesia (*adequacy level*) atau didukung dengan perjanjian yang mengikat dan memadai.
- d) Dalam hal kedua persyaratan tersebut tidak dapat dipenuhi maka diperlukan persetujuan dari Subjek Data Pribadi sebagai syarat transfer ke luar wilayah Indonesia.

6) Penghapusan dan Pemusnahan

- a) Penghapusan atau pemusnahan Data Pribadi dilakukan jika data tidak lagi diperlukan, terjadi penghentian pemrosesan, permintaan Subjek Data Pribadi, data diperoleh atau diproses secara melawan hukum, atau masa retensi telah berakhir.
- b) Proses penghapusan didahului oleh penelaah, dokumentasi Keputusan, pemisahan data yang akan dihapus, dan pemberitahuan kepada semua pihak terkait.
- c) Bukti penghapusan juga harus disampaikan kepada Subjek Data Pribadi.
- d) Pemusnahan Data Pribadi dilakukan secara aman, baik elektronik maupun nonelektronik, dan didokumentasikan sesuai ketentuan, termasuk jika permintaan dari Subjek Data Pribadi atau keputusan pengadilan.
- e. Mencatat, merekam, dan/atau mendokumentasikan aktivitas pemrosesan dan aliran Data Pribadi sesuai dengan lingkup kewenangannya.
- f. Memastikan diakomodasinya ketentuan Pelindungan Data Pribadi dalam pengelolaan data dan sistem informasi,

perjanjian kerja sama atau produk hukum yang melibatkan unit kerja.

- g. Memastikan upaya peningkatan kesadaran dan budaya Perlindungan Data Pribadi kepada sumber daya manusia di lingkungan unit kerja.
- h. Memfasilitasi pemenuhan hak Subjek Data Pribadi yang dilaksanakan sesuai jangka waktu pemenuhan sebagaimana diatur dalam UU PDP, yaitu meliputi hak:

No.	Hak Subjek Data Pribadi	Bentuk dan Jangka Waktu Pemenuhan
1.	mendapatkan Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi	disampaikan pada saat pemrosesan Data Pribadi akan dilaksanakan
2.	melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi tentang dirinya sesuai dengan tujuan pemrosesan Data Pribadi	Dipenuhi paling lambat 3 x 24 jam (tiga kali dua puluh empat jam) terhitung sejak Pengendali Data Pribadi menerima permintaan pembaruan dan/atau perbaikan Data Pribadi
3.	mendapatkan akses dan memperoleh salinan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan	dipenuhi paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak Pengendali Data Pribadi menerima permintaan akses

4.	mengakhiri pemrosesan, menghapus, dan/atau memusnahkan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.	tidak terdapat jangka waktu pemenuhan
5.	menarik kembali persetujuan pemrosesan Data Pribadi tentang dirinya yang telah diberikan kepada Pengendali Data Pribadi	tidak terdapat jangka waktu pemenuhan, namun wajib ditindaklanjuti dengan penghentian pemrosesan Data Pribadi
6.	menghentikan pemrosesan Data Pribadi dalam hal Subjek Data Pribadi menarik kembali persetujuan pemrosesan Data Pribadi	paling lambat 3 x 24 (tiga kali dua puluh empat) jam
7.	mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis, termasuk pemprofilan, yang menimbulkan akibat hukum atau berdampak signifikan pada Subjek Data Pribadi	tidak terdapat jangka pemenuhan
8.	menunda atau membatasi pemrosesan Data Pribadi secara proporsional sesuai	paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak Pengendali Data Pribadi menerima

	dengan tujuan pemrosesan Data Pribadi	permintaan penundaan dan pembatasan pemrosesan Data Pribadi
9.	meminta penghapusan atau pemusnahan Data Pribadi miliknya	tidak terdapat jangka waktu pemenuhan
10.	Menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan	tidak terdapat jangka waktu pemenuhan
11.	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	tidak terdapat jangka waktu pemenuhan
12.	menggunakan dan mengirimkan Data Pribadi tentang dirinya ke Pengendali Data Pribadi lainnya, sepanjang sistem yang digunakan dapat saling berkomunikasi secara aman sesuai dengan prinsip PDP berdasarkan UU PDP	tidak terdapat jangka waktu pemenuhan

13.	mendapatkan pemberitahuan tertulis dalam hal terjadi Kegagalan PDP kepada Subjek Data Pribadi	paling lambat 3 x 24 (tiga kali dua puluh empat) jam sejak diketahui peristiwa kegagalan Pelindungan Data Pribadi
-----	---	---

Namun dalam pelaksanaan pemenuhan hak Subjek Data Pribadi tersebut, UU PDP juga telah mengatur hak Subjek Data Pribadi yang wajib ditolak dan dapat dikecualikan. Permohonan pemenuhan hak Subjek Data Pribadi untuk memberikan akses perubahan terhadap Data Pribadi kepada Subjek Data Pribadi wajib ditolak dalam hal akibat dari akses perubahan tersebut:

- 1) membahayakan keamanan, kesehatan fisik, atau kesehatan mental Subjek Data Pribadi dan/atau orang lain;
- 2) berdampak pada pengungkapan Data Pribadi milik orang lain; dan/atau
- 3) bertentangan dengan kepentingan pertahanan dan keamanan nasional.

Sedangkan hak Subjek Data Pribadi dapat dikecualikan pemenuhannya terkait dengan:

- 1) kepentingan pertahanan dan keamanan nasional;
- 2) kepentingan proses penegakan hukum;
- 3) kepentingan umum dalam rangka penyelenggaraan negara;
- 4) kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara;
- 5) kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara; dan/atau
- 6) kepentingan statistik dan penelitian ilmiah.

i. Memastikan keamanan pemrosesan Data Pribadi

- 1) Dalam rangka memastikan keamanan pemrosesan Data Pribadi untuk mencegah kegagalan Pelindungan Data Pribadi, setiap unit kerja di lingkungan Diskomdigi melaksanakan berbagai upaya pengamanan yang selaras

dengan tugas dan fungsinya masing-masing disebabkan akibat:

- a) kegagalan kepatuhan pihak ketiga
memastikan semua kontrak dengan pihak ketiga/vendor (Prosesor Data Pribadi) mencakup perjanjian pemrosesan data (*data processing agreement*) yang mensyaratkan kepatuhan terhadap UU PDP dan standar keamanan yang setara dengan standar nasional.
- b) kegagalan pengamanan fisik dan media nonelektronik
memastikan penerapan pengamanan lingkungan fisik Data. Menetapkan kebijakan kontrol akses fisik yang ketat terhadap ruang penyimpanan data dan menetapkan prosedur standar pemusnahan Data Pribadi dalam bentuk dokumen fisik yang aman dan tidak dapat direkonstruksi.
- c) kegagalan keamanan sumber daya manusia/pegawai
melaksanakan program pelatihan kesadaran keamanan siber dan Pelindungan Data Pribadi sebagai agenda wajib tahunan bagi seluruh pegawai untuk memitigasi risiko *human error* dan meningkatkan pemahaman mengenai ancaman siber.

2) Keamanan pemrosesan Data Pribadi merupakan upaya memastikan tidak terjadinya kegagalan Pelindungan Data Pribadi, yaitu kegagalan melindungi Data Pribadi seseorang dalam hal:

- a) kegagalan menjamin kerahasiaan Data Pribadi
unit kerja memastikan bahwa akses terhadap Data Pribadi hanya diberikan kepada pihak yang berwenang dan setiap pegawai wajib menjaga kerahasiaannya dalam bentuk lisan, tertulis, maupun elektronik.
- b) kegagalan menjamin integritas Data Pribadi
unit kerja memastikan bahwa setiap perubahan atau pemutakhiran Data Pribadi dilakukan secara sah, terdokumentasi, dan melalui prosedur yang menjamin keakuratan dan keutuhannya.

- c) kegagalan menjamin ketersediaan Data Pribadi
unit kerja memastikan Data Pribadi selalu tersedia dan dapat digunakan ketika diperlukan melalui penyimpanan yang aman, pencadangan berkala, serta langkah pemulihan saat terjadi gangguan.
 - d) Kegagalan mengantisipasi pelanggaran keamanan baik yang disengaja maupun tidak disengaja, yang mengarah pada kerusakan, kehilangan, perubahan, pengungkapan, atau akses yang tidak sah terhadap Data Pribadi yang dikirim, disimpan, atau diproses.
- 3) Dalam melaksanakan upaya pengamanan dimaksud, unit kerja merujuk pada sistem manajemen keamanan informasi yang berlaku di lingkungan Diskomdigi.
 - 4) Unit kerja juga memastikan bahwa setiap potensi insiden keamanan terhadap Data Pribadi dicegah melalui langkah pengendalian yang memadai, dan apabila insiden terjadi maka seluruh pegawai wajib segera melaporkan serta menanganinya secara terkoordinasi sesuai prosedur penanganan insiden untuk meminimalkan dampak dan mencegah kejadian berulang.
 - 5) Dalam hal terjadi insiden atau kegagalan Pelindungan Data Pribadi, maka unit kerja melapor insiden dimaksud ke Tim Tanggap Insiden Siber Provinsi Jawa Tengah dalam waktu 1x24 jam (satu kali dua puluh empat) jam untuk kemudian dilakukan analisis dan pelaporan lebih lanjut ke lembaga yang menyelenggarakan Pelindungan Data Pribadi sebagaimana dimaksud dalam UU PDP, termasuk Subjek Data Pribadi sebelum batas waktu 3x24 (tiga kali dua puluh empat) jam habis.
- j. Meminta saran kepada Pejabat atau Petugas Pelindungan Data Pribadi.

F. Penutup

Pedoman Pelindungan Data Pribadi ini disusun untuk memberikan arahan yang jelas dan terukur bagi seluruh unit kerja di lingkungan

Diskomdigi dalam melaksanakan pengelolaan Data Pribadi. Dengan adanya pedoman ini, setiap unit kerja memiliki rujukan normatif dan operasional untuk memastikan bahwa aktivitas pemrosesan Data Pribadi berjalan sesuai dengan prinsip perlindungan, kepatuhan hukum, serta standar tata kelola yang baik.

KEPALA DINAS KOMUNIKASI, INFORMATIKA, DAN DIGITAL
PROVINSI JAWA TENGAH



LILIK HENRY RISTANTO