**PEMERINTAH KABUPATEN KENDAL**
**SEKRETARIAT DAERAH**
Jl. Soekarno – Hatta No. 193 Kendal Telp. Fax. (0294) 381232 Kode Pos 51311
e-mail : setda@kendalkab.go.id website : setda.kendalkab.go.id

SEKRETARIS DAERAH KABUPATEN KENDAL

KEPUTUSAN SEKRETARIS DAERAH KABUPATEN KENDAL

NOMOR : 100.3.3.5/2280/2025

TENTANG

PROSEDUR PENGENDALIAN PELINDUNGAN DATA PRIBADI DI LINGKUNGAN PEMERINTAH KABUPATEN KENDAL

SEKRETARIS DAERAH KABUPATEN KENDAL,

Menimbang :
a. bahwa dalam rangka menyelenggarakan tata kelola pemerintahan digital yang aman, akuntabel, dan terpercaya di lingkungan Pemerintah Kabupaten Kendal, diperlukan pelindungan menyeluruh terhadap hak atas privasi dan data pribadi milik masyarakat maupun aparatur sipil negara;
b. bahwa dalam rangka melaksanakan ketentuan operasional penanganan data pribadi, diperlukan petunjuk teknis yang baku dan mengikat;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, maka perlu menetapkan Keputusan Sekretaris Daerah tentang Prosedur Pengendalian Pelindungan Data Pribadi di Lingkungan Pemerintah Kabupaten Kendal;

Mengingat :
1. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Djawa Tengah sebagaimana telah diubah dengan Undang-Undang Nomor 9 Tahun 1965 tentang Pembentukan Daerah Tingkat II Batang dengan Mengubah Undang- Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Jawa Tengah (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 52, Tambahan Lembaran Negara Republik Indonesia Nomor 2757);
2. 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 diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
3. 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 beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana (Lembaran Negara Republik Indonesia Tahun 2026 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 7153);

4. 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);
5. Peraturan Pemerintah Nomor 32 Tahun 1950 tentang Penetapan mulai Berlakunya Undang-Undang 1950 Nomor 12, 13, 14 dan 15 dari Hal Pembentukan Daerah-daerah Kabupaten di Jawa Timur/Tengah/Barat dan Daerah Istimewa Yogyakarta;
6. Peraturan Pemerintah Nomor 16 Tahun 1976 tentang Perluasan Kotamadya Daerah Tingkat II Semarang (Lembaran Negara Republik Indonesia Tahun 1976 Nomor 25, Tambahan Lembaran Negara Republik Indonesia Nomor 3079);
7. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2018 Nomor 182, Tambahan Berita Negara Republik Indonesia Nomor 4843);
8. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Berita Negara Republik Indonesia Tahun 2022 Nomor 129);
9. Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (Berita Negara Republik Indonesia Tahun 2023 Nomor 99);
10. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber (Berita Negara Republik Indonesia Tahun 2024 Nomor 43);
11. Peraturan Bupati Kendal Nomor 35 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kendal (Berita Daerah Kabupaten Kendal Tahun 2021 Nomor 35) sebagaimana telah diubah dengan Peraturan Bupati Kendal Nomor 33 Tahun 2024 tentang Perubahan Atas Peraturan Bupati Kendal Nomor 35 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kendal Berita Daerah Kabupaten Kendal Tahun 2024 Nomor 34);
12. Peraturan Bupati Kendal Nomor 57 Tahun 2023 tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kendal (Berita Daerah Kabupaten Kendal Tahun 2023 Nomor 57);

MEMUTUSKAN:

Menetapkan :

KESATU : Prosedur Pengendalian Pelindungan Data Pribadi di Lingkungan Pemerintah Kabupaten Kendal sebagaimana tercantum dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Keputusan ini.

KEDUA : Prosedur Pengendalian Pelindungan Data Pribadi di Lingkungan Pemerintah Kabupaten Kendal sebagaimana dimaksud diktum KESATU digunakan sebagai memberikan pedoman operasional

yang terstruktur, baku, dan akuntabel Pemerintah Kabupaten Kendal dalam mengelola siklus hidup data pribadi; menjamin pemenuhan hak-hak pemilik data pribadi; serta menerapkan standar pengamanan teknis berbasis risiko.

KETIGA : Segala biaya yang timbul sebagai akibat ditetapkannya Keputusan ini dibebankan pada Anggaran Pendapatan dan Belanja Daerah Kabupaten Kendal.

KEEMPAT : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Kendal
pada tanggal 28 oktober 2025

Pj. SEKRETARIS DAERAH
KABUPATEN KENDAL,

AGUS DWI LESTARI

SALINAN : Keputusan ini disampaikan kepada Yth :
1. Segenap Agen Siber yang bersangkutan; dan
2. Arsip.

LAMPIRAN
KEPUTUSAN SEKRETARIS DAERAH
KABUPATEN KENDAL
NOMOR : 100.3.3.5/2280/2025
TANGGAL : 28 OKTOBER 2025

**PROSEDUR PENGENDALIAN PELINDUNGAN DATA PRIBADI DI LINGKUNGAN PEMERINTAH KABUPATEN KENDAL**

**DAFTAR ISTILAH**

| Istilah/Singkatan | Definisi |
|---|---|
| *Right to be Forgotten* | Hak Subjek Data untuk meminta penghentian pemrosesan, penghapusan, dan/atau pemusnahan data pribadi miliknya dari sistem Pengendali Data Pribadi sepanjang tidak bertentangan dengan ketentuan peraturan perundang-undangan |
| *Consent* | Persetujuan yang sah, jelas, dan transparan dari Subjek Data secara tertulis atau terekam untuk memproses data pribadinya sesuai tujuan yang telah diinformasikan |
| *Data Protection Officer* (DPO) | Pejabat atau tim yang ditunjuk oleh Pengendali Data Pribadi untuk mengawasi kepatuhan pelindungan data pribadi, memberikan rekomendasi/saran, serta menjadi titik kontak utama (*liaison*) antara organisasi, masyarakat, dan Otoritas Pelindungan Data |
| *Data Protection Impact Assessment* (DPIA) | Kajian Dampak Pelindungan Data Pribadi (KDPDP), yaitu proses analisis dan evaluasi sistematis untuk mengidentifikasi, menilai, dan memitigasi potensi risiko pelanggaran privasi atau kegagalan pelindungan data sebelum suatu layanan/sistem digital baru diimplementasikan |
| *Personal/Household Activities* | Kegiatan pribadi atau rumah tangga individu di luar ranah kedinasan, operasional resmi, atau tugas publik organisasi yang dikecualikan dari ruang lingkup prosedur pengendalian pelindungan data pribadi |
| *Data Masking* | Teknik pengamanan dengan menyamarkan atau mengganti karakter data pribadi sensitif menggunakan karakter artifisial sehingga nilai aslinya tidak dapat dilihat langsung, terutama pada lingkungan pengujian sistem atau analisis data |
| *Data Leakage Prevention* (DLP) | Teknologi atau perangkat pengamanan teknis yang berfungsi mendeteksi, memantau, dan mencegah pemindahan atau kebocoran data pribadi ke luar jaringan organisasi secara tidak sah |
| *Incident Management* | Rangkaian prosedur dan penanganan sistematis untuk mendeteksi, menganalisis, mengisolasi, dan memulihkan sistem dari gangguan atau kegagalan keamanan informasi/kebocoran data |

| | |
|---|---|
| *Access Rights/Access Control* | Pembatasan dan pengaturan hak akses pengguna ke sistem atau data pribadi berdasarkan peran dan kewenangan operasionalnya |
| *Need-to-Know* | Prinsip pembatasan akses di mana pegawai hanya diberikan akses terhadap data pribadi yang benar-benar dibutuhkan untuk melaksanakan tugas dan fungsi jabatannya |
| *Least Privilege* | Kebijakan pemberian hak akses minimal yang diperlukan oleh pengguna atau sistem untuk menjalankan fungsinya guna meminimalkan risiko keamanan |
| *Privacy by Design* | Pendekatan rekayasa sistem yang mengintegrasikan prinsip-prinsip pelindungan privasi dan data pribadi sejak awal tahap perancangan dan arsitektur aplikasi/sistem informasi |
| *Privacy by Default* | Prinsip yang menjamin bahwa setelan keamanan dan privasi tertinggi diterapkan secara otomatis pada suatu aplikasi atau sistem tanpa memerlukan konfigurasi tambahan dari pengguna |
| *Service Level Agreement* (SLA) | Perjanjian tingkat layanan antara Pengendali Data (Perangkat Daerah) dan Prosesor Data (Pihak Ketiga) yang mengatur standar performa, keandalan, dan pengamanan sistem |
| *Data Minimization* | Asas minimisasi data, yaitu prinsip pembatasan pengumpulan data pribadi sebatas informasi yang relevan, memadai, dan benar-benar diperlukan sesuai tujuan pemrosesan |
| *Data Flow Mapping* | Pemetaan visual atau deskriptif mengenai seluruh alur perjalanan data pribadi, mulai dari perolehan, pengolahan, penyimpanan, transfer, hingga pemusnahan |
| *Data Flow Diagram* (DFD) | Diagram alur data yang menggambarkan secara teknis bagaimana data pribadi masuk ke dalam sistem, diolah oleh proses internal, ditransfer ke pihak eksternal, dan disimpan di media basis data |
| *Retention Period* | Jangka waktu retensi atau batas durasi maksimal penyimpanan data pribadi sebelum data wajib dihapus, dimusnahkan, atau dianonimkan |
| *Privacy Notice* | Pemberitahuan atau maklumat privasi yang disampaikan secara transparan kepada Subjek Data mengenai tujuan pengumpulan, penggunaan, penyimpanan, dan hak-hak mereka atas data pribadi |
| *Unauthorized Insider Access* | Potensi atau tindakan penyalahgunaan akses data pribadi oleh pihak internal/pegawai yang tidak memiliki wewenang sah |
| *Risk Reduction* | Tindakan dan langkah konkret untuk menurunkan tingkat risiko keamanan informasi hingga mencapai batas yang dapat diterima oleh organisasi |

| | |
|---|---|
| *Non-Disclosure Agreement* (NDA) | Perjanjian atau klausul kerahasiaan hukum yang mengikat pihak-pihak terkait untuk tidak membocorkan atau mengungkapkan data pribadi/informasi rahasia kepada pihak lain |
| *Business Impact Analysis* (BIA) | Analisis dampak bisnis/operasional untuk menilai sejauh mana potensi kerugian dan gangguan yang timbul akibat terjadinya insiden keamanan atau kegagalan sistem |
| *Likelihood* | Evaluasi atau tingkat kemungkinan terjadinya suatu insiden keamanan siber atau pelanggaran data pribadi dalam kurun waktu tertentu |
| *Accountability Principle* | Asas akuntabilitas yang mewajibkan Pengendali Data Pribadi untuk membuktikan secara hukum dan teknis bahwa seluruh pemrosesan data telah mematuhi aturan pelindungan data |
| Tokenisasi (*Tokenization*) | Metode pengamanan data dengan mengganti elemen data sensitif menggunakan simbol/token acak yang tidak bernilai tanpa menggunakan kunci pemutus (*decryption key*) |
| *Data at Rest* | Data pribadi yang sedang disimpan secara permanen atau sementara di dalam media penyimpanan digital (seperti *database*, *server*, atau *cloud*) |
| *Data in Transit* | Data pribadi yang sedang mengalir atau ditransmisikan melalui infrastruktur jaringan (seperti internet, intranet, atau fiber optik) |
| *Pseudonimisasi* | Pemrosesan data pribadi sedemikian rupa sehingga data tersebut tidak lagi dapat dihubungkan dengan Subjek Data tanpa menggunakan informasi tambahan yang disimpan secara terpisah |
| *Multi-Factor Authentication* (MFA) | Mekanisme autentikasi keamanan yang mengharuskan pengguna memberikan dua atau lebih bukti verifikasi identitas (misal: *password* + kode OTP) sebelum mendapatkan akses ke dalam sistem |
| *Log Audit/Audit Trail* | Catatan kronologis otomatis yang merekam seluruh aktivitas pembuatan, pembacaan, pengubahan, dan penghapusan (CRUD) terhadap data pribadi di dalam sistem informasi |
| *Vendor Security Assessment* | Proses evaluasi dan penilaian tingkat keamanan informasi terhadap penyedia jasa/pihak ketiga sebelum dilakukan kerja sama atau transfer data |
| *Data Processing Addendum* (DPA) | Dokumen adendum atau klausul tambahan pada kontrak kerja sama yang secara spesifik mengatur kewajiban, batasan, dan pengamanan pemrosesan data oleh pihak ketiga |
| *Sub-processor* | Pihak ketiga turunan yang disewa atau ditunjuk oleh Prosesor Data utama untuk membantu pelaksanaan pemrosesan data atas persetujuan Pengendali Data |

| | |
|---|---|
| *Secure File Transfer Protocol* (SFTP) | Protokol transfer berkas aman yang menggunakan enkripsi jalur (*SSH*) untuk mengirimkan data pribadi antar server atau ke pihak ketiga |
| *Application Programming Interface* (API) | Antarmuka pemrograman aplikasi yang memungkinkan interaksi dan pertukaran data secara aman antar sistem/aplikasi menggunakan protokol terstandar |
| *Sanitization/Secure Wiping* | Metode pemusnahan atau penghapusan data digital secara permanen dari media penyimpanan sehingga data tidak dapat dipulihkan kembali (*unrecoverable*) |
| *Shredder* | Mesin penghancur dokumen fisik/kertas hingga menjadi potongan-potongan kecil guna menjamin data pribadi tidak dapat direkonstruksi kembali |
| *On-Premise* | Infrastruktur server atau pusat data yang berlokasi, dikelola, dan dioperasikan secara fisik di dalam gedung/fasilitas milik organisasi sendiri |
| *Cloud Storage* | Layanan media penyimpanan data digital yang disewa dan diakses melalui jaringan internet dari penyedia komputasi awan |

**PROSEDUR PENGENDALIAN PELINDUNGAN DATA PRIBADI DI LINGKUNGAN PEMERINTAH KABUPATEN KENDAL**

## 1. Maksud dan Tujuan

1.1. Maksud dari penyusunan prosedur pengendalian pelindungan data pribadi di lingkungan Pemerintah Kabupaten Kendal adalah untuk menyediakan sebuah kerangka kerja, standar operasional, dan panduan praktis yang mengikat bagi seluruh elemen di dalam organisasi (manajemen, karyawan, maupun mitra pihak ketiga) di lingkungan Pemerintah Kabupaten Kendal dalam memperlakukan data pribadi.

1.2. Kebijakan ini menjadi jembatan antara regulasi hukum yang bersifat makro dengan tindakan teknis sehari-hari di lapangan (mikro), sehingga tidak ada ambiguitas dalam pemrosesan data.

1.3. Kepatuhan Hukum (*Legal Compliance)*

1.3.1. memastikan organisasi tunduk dan patuh sepenuhnya terhadap kewajiban Pengendali Data Pribadi sebagaimana diatur dalam Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi dan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik;

1.3.2. menghindarkan organisasi dari sanksi administratif (seperti denda publik hingga penghentian kegiatan pemrosesan data) maupun sanksi pidana akibat kelalaian pengelolaan data pribadi.

1.4. Perlindungan Hak Subjek Data

1.4.1. memastikan hak-hak pemilik data pribadi (karyawan dan mitra layanan pemerintahan baik pihak ketiga maupun masyarakat) terpenuhi, seperti hak untuk mengakses, memperbaiki, menghapus (*right to be forgotten*), dan menarik kembali persetujuan (*consent*);

1.4.2. menjelaskan secara jujur dan transparan kepada pemilik data mengenai bagaimana data mereka dikumpulkan, digunakan, dianalisis, disimpan, hingga dimusnahkan.

1.5. Operasional dan Keamanan Informasi

1.5.1. mengatur tata cara baku pemrosesan data pribadi mulai dari perolehan, penampilan/pengumuman, pengiriman/transfer, penyimpanan, hingga penghapusan/pemusnahan;

1.5.2. menetapkan standar keamanan teknis dan keamanan organisasi untuk mencegah akses tidak sah, peretasan, atau kebocoran data.

1.6. Reputasi dan Kepercayaan Bisnis (*Public Trust*)

1.6.1. membangun citra positif bahwa organisasi memiliki tata kelola yang bertanggung jawab (good corporate governance) dan peduli terhadap privasi pelanggan atau anggotanya;

1.6.2. menentukan secara tegas peran dan tanggung jawab di internal organisasi.

**2. Ruang Lingkup**

Prosedur pengendalian pelindungan data pribadi di lingkungan Pemerintah Kabupaten Kendal berlaku meliputi:

2.1. Data pribadi yang diproses

Kebijakan ini membatasi objek pelindungannya pada seluruh Data Pribadi (baik yang dikelola oleh organisasi bertindak yang sebagai Pengendali Data Pribadi maupun Prosesor Data Pribadi) yang dibagi sesuai UU PDP menjadi:

2.1.1. Data Pribadi Bersifat Spesifik: Data kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan data lainnya yang diatur peraturan perundang-undangan;

2.1.2. Data Pribadi Bersifat Umum: Nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang;

2.1.3. Siklus Pemrosesan Data: Kebijakan ini mengikat seluruh rangkaian aktivitas terhadap objek data di atas, mulai dari tahap perolehan / pengumpulan, pengolahan / penganalisisan, penyimpanan, penampilan / pengungkapan, transfer / pengiriman, hingga penghapusan dan pemusnahan.

2.2. Subyek dan pengendali data pribadi

Kebijakan ini mengatur hak, kewajiban, dan tanggung jawab hukum dari para pihak yang terlibat dalam pemrosesan data, meliputi:

2.2.1. Subyek Data Pribadi (Pemilik Data):

Seluruh individu yang datanya diproses oleh organisasi, termasuk namun tidak terbatas pada: pegawai (ASN/ tetap/ kontrak), pengguna layanan masyarakat/pelanggan, masyarakat umum, serta personel dari mitra/pihak ketiga;

2.2.2. Pengendali Data Pribadi (Organisasi):

Organisasi bertindak sebagai Pengendali Data Pribadi yang menetapkan tujuan dan melakukan kendali atas pemrosesan data pribadi, termasuk jajaran manajemen, pimpinan, dan pejabat/unit kerja yang ditunjuk (seperti Pejabat Pelindung Data/DPO);

2.2.3. Prosesor Data Pribadi (Pihak Ketiga):

Setiap orang, badan publik, atau organisasi internasional yang bertindak sendiri atau bersama-sama dalam melakukan pemrosesan data pribadi atas nama organisasi (misalnya: vendor IT, penyedia layanan outsourcing, konsultan, dan mitra strategis).

2.3. Media dan Sistem Pengolah Data Pribadi

Kebijakan ini berlaku untuk semua jenis media, lingkungan kerja, dan sistem informasi yang digunakan sebagai wadah atau sarana pemrosesan data pribadi, yang mencakup:

2.3.1. Sistem Elektronik (Digital):

2.3.1.1. Seluruh aplikasi internal, sistem informasi administrasi pemerintahan/bisnis, platform layanan publik digital, dan situs web resmi organisasi;

2.3.1.2. Basis data (*database*), server lokal (*on-premise*), pusat data (*data center*), serta komputasi awan (*cloud storage*) yang disewa atau dikelola organisasi;

2.3.1.3. Seluruh lalu lintas data yang mengalir melalui infrastruktur jaringan organisasi (kabel, fiber optic, maupun radio/nirkabel) saat data ditransmisikan.

2.3.2. Media Non-Elektronik (Fisik):
Dokumen cetak, formulir kertas, berkas administrasi fisik, lembar disposisi, arsip negara, serta dokumen fisik lainnya yang memuat data pribadi.

2.3.3. Lingkungan Keamanan Fisik:
Ruang server, ruang arsip, ruang kerja pegawai, dan fasilitas gedung organisasi yang menjadi tempat penyimpanan atau pemrosesan media elektronik maupun non-elektronik tersebut.

2.4. Pengecualian (*Out of Scope*)
Kebijakan ini tidak berlaku untuk pemrosesan data pribadi yang dilakukan oleh individu/pegawai untuk kegiatan pribadi atau rumah tangga (personal/*household activities*) yang berada di luar ranah kedinasan/operasional resmi organisasi, atau data yang telah melalui proses anonimisasi secara permanen sehingga tidak dapat diidentifikasi kembali.

## 3. Referensi

3.1. ISO/IEC 27001:2022 – Annex A.5.34 Privacy and Protection of Personally Identifiable Information
3.2. ISO/IEC 27001:2022 – Annex A.5.18 Access rights
3.3. ISO/IEC 27001:2022 – Annex A.5.24 s.d A.5.28 - Information security incident management
3.4. ISO/IEC 27001:2022 – Annex A.8.11 - Data masking
3.5. ISO/IEC 27001:2022 – Annex A.8.12 - Data leakage prevention

## 4. Peran dan Tanggung Jawab

4.1. Bupati Kendal selaku Penanggung Jawab Badan Publik Daerah Kabupaten Kendal bertanggung jawab menetapkan regulasi daerah mengenai pelindungan data pribadi di lingkungan Pemerintah Kabupaten Kendal, bertanggung jawab secara hukum sebagai pucuk pimpinan Badan Publik yang bertindak selaku Pengendali Data Pribadi, dan menunjuk Koordinator Pelindungan Data Pribadi Pemerintah Kabupaten Kendal.

4.2. Koordinator Pelindungan Data Pribadi Pemerintah Kabupaten Kendal dalam hal ini dijabat oleh Sekretaris Daerah Kabupaten Kendal selaku Koordinator Pemerintahan Digital Kabupaten Kendal bertanggung jawab untuk memastikan penyelenggaraan pelindungan data pribadi di Pemerintah Kabupaten Kendal, memastikan alokasi anggaran dan sumber daya yang memadai untuk implementasi pelindungan data pribadi dan menunjuk Tim Pelindungan Data (*Data Protection Officer* – DPO).

4.3. Tim Pelindungan Data (*Data Protection Office* – DPO) dalam hal ini dikoordinasikan oleh Kepala Dinas Komunikasi dan Informatika Kabupaten Kendal bertanggung jawab untuk:

4.3.1. mengawasi dan memastikan seluruh Perangkat Daerah mematuhi kebijakan internal Pelindungan Data Pribadi dan peraturan perundang-undangan yang berlaku;

4.3.2. memberikan saran dan rekomendasi dalam penyusunan *Data Protection Impact Assessment* (DPIA) atau Kajian Dampak Pelindungan Data jika perangkat daerah sebagai pemilik proses bisnis akan meluncurkan layanan digital baru;

4.3.3. menjadi titik kontak utama (*liaison*) antara Pemerintah Daerah dengan Lembaga Otoritas Pelindungan Data Pribadi Nasional maupun dengan masyarakat (Subjek Data).

4.4. Perangkat Daerah Kabupaten Kendal selaku pemilik proses bisnis sekaligus pengendali data pribadi bertanggung jawab untuk:

4.4.1. melaksanakan pemrosesan data spesifik (misalnya: Dinas Dukcapil untuk data kependudukan, Dinas Kesehatan untuk data rekam medis, BKD/BKPSDM untuk data kepegawaian);

4.4.2. memastikan perolehan data pribadi dari masyarakat didasarkan pada persetujuan (consent) yang sah, jelas, dan transparan secara hukum;

4.4.3. menerapkan pembatasan hak akses (*access control*) internal pegawai berdasarkan asas *need-to-know* (hanya pegawai yang bertugas yang bisa melihat data);

4.4.4. memastikan proses data dilaksanakan sesuai ketentuan yang berlaku dan mencantumkannya ke dalam kontrak kerja sama (PKS/SLA) apabila proses data dilakukan oleh pihak ketiga (Vendor IT, Konsultan, Penyedia Jaringan);

4.4.5. menyusun draf dokumen *Data Protection Impact Assessment* (DPIA) atau Kajian Dampak Pelindungan Data sebelum sistem elektronik atau program layanan baru tersebut diimplementasikan;

4.4.6. Melaporkan segera (paling lambat dalam hitungan jam) ke *Data Protection Office* – DPO jika mendeteksi adanya anomali atau indikasi kebocoran data di aplikasinya.

4.5. Tim Tanggap Insiden Siber Kabupaten Kendal selaku penyelenggara operasional penanggulangan insiden siber dan keamanan informasi bertanggung jawab untuk:

4.5.1. menyelenggarakan mitigasi dan pencegahan kebocoran data dengan pemeriksaan celah keamanan pada sistem yang mengelola data pribadi, penyebaran diseminasi dan peringatan dini tentang tren ancaman siber, dan penyelenggaraan audit keamanan informasi;

4.5.2. menangani insiden kebocoran data sebagai penanggulangan dengan analisis sumber dan dampak dari serangan atau peretasan data, mencegah perluasan dampak kerusakan atas serangan atau peretasan data, memperbaiki sistem yang rusak akibat peretasan dan mengembalikan data ke kondisi aman;

4.5.3. memberikan data teknis akurat tentang insiden kepada pengelola sistem (pengendali data) untuk dilaporkan ke pihak berwenang dan bekerja sama dengan pihak penegak hukum atau lembaga pengawas terkait.

4.6. Pihak Ketiga (Vendor IT, Konsultan, Penyedia Jaringan) selaku prosesor Data Pribadi (Pihak yang memproses data atas nama Pemerintah Kabupaten Kendal) bertanggung jawab untuk:

4.6.1. memproses data pribadi masyarakat/pegawai secara ketat hanya sesuai dengan instruksi tertulis dalam kontrak kerja sama (PKS/SLA) dengan pemilik proses bisnis atau dalam hal ini Perangkat Daerah Kabupaten Kendal;

4.6.2. menjamin sistem atau aplikasi yang mereka bangun untuk pemilik proses bisnis atau dalam hal ini Perangkat Daerah Kabupaten Kendal telah mengadopsi prinsip *Privacy by Design* dan *Privacy by Default*;

4.6.3. ikut bertanggung jawab secara hukum dan finansial jika kebocoran data terjadi akibat kegagalan sistem atau kelalaian teknis yang dikelola.

4.7. Masyarakat selaku subyek data dan pemilik sah data pribadi berkewajiban untuk memberikan data yang sahih dan ikut menjaga keamanan akun/kredensial layanan digital mereka sendiri (tidak memberikan OTP/password kepada pihak lain) dan berhak untuk:

4.7.1. mendapatkan informasi transparan mengenai tujuan pengumpulan data oleh layanan yang diselenggarakan oleh Pemerintah Kabupaten Kendal;

4.7.2. mengajukan keberatan, meminta perbaikan data yang keliru, hingga meminta penghapusan data (sesuai ketentuan hukum, yang dikecualikan arsip negara).

## 5. Kebijakan Umum

5.1. Landasan Prinsip Pemrosesan Data Pribadi

Organisasi menetapkan bahwa setiap aktivitas pemrosesan data pribadi wajib mematuhi asas legalitas dan akuntabilitas, yang meliputi:

5.1.1. data pribadi hanya dikumpulkan untuk tujuan yang spesifik, sah secara hukum, dan transparan bagi Subjek Data;

5.1.2. pengumpulan data pribadi harus dibatasi hanya pada informasi yang relevan, memadai, dan terbatas pada apa yang diperlukan untuk mencapai tujuan pemrosesan (*data minimization*);

5.1.3. organisasi wajib memastikan data pribadi yang dikelola akurat, lengkap, tidak menyesatkan, dan diperbarui secara berkala;

5.1.4. data pribadi hanya disimpan selama diperlukan sesuai dengan tujuan pemrosesan atau berdasarkan batas waktu yang diwajibkan oleh peraturan perundang-undangan.

5.2. Legalitas Pemrosesan

5.2.1. persetujuan (*consent*) yang sah, eksplisit, dan tertulis/terekam dari Subjek Data;

5.2.2. pemenuhan kewajiban perjanjian/kontrak di mana Subjek Data merupakan salah satu pihak;
5.2.3. pemenuhan kewajiban hukum Pengendali Data Pribadi berdasarkan peraturan perundang-undangan yang berlaku;
5.2.4. pemenuhan kepentingan umum dalam rangka penyelenggaraan tugas negara/pelayanan publik.

5.3. Tata Kelola dan Keamanan Organisasi
5.3.1. Organisasi menunjuk Tim Pelindungan Data (*Data Protection Officer* - DPO) yang independen untuk mengawasi kepatuhan PDP, memberikan saran, dan menjadi titik kontak utama bagi otoritas pengawas;
5.3.2. Setiap pengembangan sistem informasi baru, aplikasi, atau proses bisnis yang melibatkan pemrosesan data pribadi berisiko tinggi wajib melalui proses *Data Protection Impact Assessment* (DPIA) sebelum diluncurkan;

5.4. Organisasi wajib melakukan Kajian Dampak Pelindungan Data Pribadi (KDPDP) atau *Data Protection Impact Assessment* (DPIA) terhadap setiap rencana pemrosesan data pribadi yang memiliki potensi risiko tinggi terjadinya pelanggaran privasi atau kegagalan pelindungan data.

5.5. Kajian Dampak Pelindungan Data Pribadi (KDPDP) atau *Data Protection Impact Assessment* (DPIA)
5.5.1. Ambang batas penyusunan Kajian Dampak Pelindungan Data Pribadi atau Data Protection Impact Assesment, organisasi harus memastikan kriteria pemicu pemrosesan berisiko tinggi dipenuhi, antara lain:
5.5.1.1. pemrosesan data pribadi bersifat otomatis yang berdampak signifikan pada Subjek Data (misal: *profiling* kredit/bantuan sosial, *profiling* ketentuan kenaikan pangkat pada sistem kepegawaian, *profiling* izin usaha, izin penelitian, dan lain sebagainya);
5.5.1.2. pemrosesan data pribadi bersifat spesifik/sensitif dalam skala besar (data kesehatan, biometrik, kepegawaian, data anak, riwayat pelanggaran hukum, dan lain sebagainya);
5.5.1.3. pemrosesan data untuk pemantauan sistematis area publik skala luas (misal: CCTV cerdas/analitik berbasis *face recognition*);
5.5.1.4. penggunaan teknologi baru yang belum teruji dampaknya terhadap privasi masyarakat.
5.5.2. Perangkat penyusun kajian menjelaskan keseluruhan mengenai deskripsi sistem dan pemetaan siklus data (*data flow mapping*) setidak-tidaknya mencantumkan:
5.5.2.1. Tujuan dan Dasar Hukum Pemrosesan:
Alasan bisnis/pelayanan publik serta dasar hukumnya (persetujuan, kewajiban undang-undang, atau kepentingan umum).
5.5.2.2. Inventarisasi Data:

Rincian jenis data pribadi yang dikumpulkan, kategori Subjek Data, dan sumber perolehan data.

5.5.2.3. Diagram Alur Data (*Data Flow Diagram*):
Pemetaan jelas bagaimana data masuk, diolah, ditransfer ke pihak lain, disimpan, hingga dimusnahkan.

5.5.3. Memastikan pemrosesan data dilakukan secara tidak berlebihan dengan menerapkan:

5.5.3.1. Asas Minimisasi:
Bukti bahwa data yang dikumpulkan benar-benar sebatas yang dibutuhkan (*need-to-have*, bukan *nice-to-have*).

5.5.3.2. Ketentuan Retensi:
Penetapan masa simpan yang jelas (*retention period*) dan skema pemusnahannya setelah batas waktu berakhir.

5.5.3.3. Transparansi:
Mekanisme pemberitahuan privasi (*privacy notice*) kepada Subjek Data.

5.5.4. Identifikasi potensi bahaya dari sudut pandang masyarakat/pemilik data dengan parameter:

5.5.4.1. Ancaman Kerahasiaan & Keutuhan:
Risiko kebocoran data, pencurian identitas, peretasan, atau manipulasi data.

5.5.4.2. Dampak Kerugian Subjek Data:
Risiko diskriminasi, kerugian finansial, kerugian reputasi, hingga hilangnya kontrol atas data pribadi mereka.

5.5.4.3. Potensi Akses Tanpa Hak:
Risiko penyalahgunaan akses internal oleh pegawai (*unauthorized insider access*).

5.5.5. Menentukan langkah konkret untuk menurunkan tingkat risiko (*risk reduction*) dengan parameter:

5.5.5.1. Penerapan enkripsi (*data at rest* dan *in transit*), penyamaran data (data masking), pembatasan akses (*access control*), dan pencegahan kebocoran (DLP).

5.5.5.2. Penyusunan SOP pemrosesan data, pelatihan kepatuhan pegawai, dan klausul kerahasiaan (NDA) dengan pihak ketiga.

5.5.5.3. Penyediaan fitur/kanal operasional bagi Subjek Data untuk mengakses, memperbaiki, atau menghapus data mereka.

5.6. Pemrosesan data pribadi yang dikategorikan memiliki potensi risiko tinggi sebagaimana dimaksud di atas meliputi:

5.6.1. pemrosesan data pribadi yang bersifat spesifik (termasuk data kesehatan, data biometrik, catatan kejahatan, dan data keuangan pribadi) dalam skala besar;

5.6.2. pemanfaatan teknologi baru, otomatisasi sistem, atau adopsi platform kecerdasan buatan (*Artificial Intelligence*) dalam memproses data pribadi;

5.6.3. penyusunan profil (*profiling*) atau evaluasi berskala besar terhadap aspek pribadi individu secara otomatis yang menghasilkan akibat hukum atau dampak signifikan bagi Subjek Data.

5.7. Proses penilaian risiko privasi wajib diintegrasikan dengan metodologi Manajemen Risiko Keamanan Informasi yang selaras dengan standar ISO/IEC 27001:2022, yang mencakup tahapan identifikasi risiko, analisis dampak risiko (*Business Impact Analysis*), serta evaluasi tingkat kemungkinan terjadinya insiden (*likelihood*).

5.7.1. deskripsi sistematis mengenai alur pemrosesan, sifat, ruang lingkup, konteks, dan tujuan pemrosesan data pribadi;

5.7.2. penilaian terhadap urgensi, proporsionalitas, dan kebutuhan pemrosesan data dibandingkan dengan tujuan utamanya (*data minimization check*);

5.7.3. penilaian risiko terhadap hak-hak Subjek Data, termasuk potensi kerugian materiil maupun immateriil akibat kebocoran data; dan

5.7.4. langkah-langkah mitigasi, kendali pengamanan teknis (seperti enkripsi, tokenisasi, data masking), serta mekanisme organisasi untuk melindungi data pribadi dan membuktikan kepatuhan hukum (*accountability principle*).

5.8. Pengamanan Teknis dan Infrastruktur

5.8.1. seluruh data pribadi yang bersifat spesifik/sensitif wajib dienkripsi, baik saat disimpan di dalam basis data (data at rest) maupun saat ditransmisikan melalui jaringan internet/intranet (*data in transit*);

5.8.2. seluruh data pribadi yang ditransmisikan jaringan internet/intranet (*data in transit*) menggunakan protokol komunikasi aman;

5.8.3. Menerapkan teknik data masking atau pseudonimisasi pada data pribadi yang digunakan untuk keperluan lingkungan pengujian (*testing*), pengembangan sistem, maupun analisis statistik;

5.8.4. hak akses ke sistem yang memuat data pribadi diatur secara ketat berdasarkan asas *least privilege* dan *need-to-know*. Setiap akses wajib melalui mekanisme autentikasi yang aman (seperti *Multi-Factor Authentication*);

5.8.5. engimplementasikan sistem pemantauan lalu lintas data dan teknologi *Data Leakage Prevention* (DLP) untuk mendeteksi serta mencegah pemindahan data pribadi ke luar organisasi secara tidak sah;

5.8.6. Sistem yang mengelola dan menyimpan data pribadi wajib mencatat log audit secara otomatis untuk setiap aktivitas pembuatan, pembacaan, pengubahan, dan penghapusan (CRUD) terhadap data pribadi.

5.9. Distribusi Data Pribadi ke Pihak Ketiga

5.9.1. Sebelum melakukan transfer atau berbagi Data Pribadi dengan pihak ketiga (mitra, vendor, atau prosesor data eksternal), wajib dilakukan penilaian risiko keamanan informasi (vendor security assessment) untuk memastikan pihak ketiga memiliki kapabilitas perlindungan data yang setara;

5.9.2. Setiap distribusi data ke pihak ketiga wajib diikat dengan Perjanjian Pemrosesan Data/*Document Processing Addendum* (DPA) atau klausul pelindungan data yang tegas di dalam kontrak kerja sama, yang setidak-tidaknya memuat:

5.9.2.1. tujuan spesifik transfer data;

5.9.2.2. kewajiban pihak ketiga untuk menjaga kerahasiaan dan menerapkan kontrol keamanan;

5.9.2.3. larangan memindahtangankan data ke pihak lain (*sub-processor*) tanpa persetujuan tertulis dari organisasi;

5.9.2.4. kewajiban melaporkan insiden kebocoran data dengan segera.

5.9.3. Pengiriman Data Pribadi ke pihak ketiga dilarang menggunakan media yang tidak aman (seperti email biasa atau aplikasi pesan instan personal). Transfer harus menggunakan jalur terenkripsi seperti SFTP (*Secure File Transfer Protocol*) atau API (*Application Programming Interface*) dengan pengamanan token yang divalidasi berkala.

## 6. Pemenuhan Hak Subjek Data

Organisasi wajib menyediakan mekanisme, kanal pengaduan, dan standar operasional yang mudah diakses oleh Subjek Data untuk memenuhi hak-hak mereka sesuai amanah Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang meliputi:

6.1. Hak mendapatkan informasi dan mengakses data pribadi sesuai dengan kepemilikannya;

6.2. Hak memperbarui, memperbaiki, dan melengkapi kekeliruan data;

6.3. Hak mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data (*right to be forgotten*) sepanjang tidak bertentangan dengan hukum negara;

6.4. Hak mengajukan keberatan atas tindakan pemrosesan berbasis otomatisasi.

## 7. Manajemen Insiden Kebocoran Data

7.1. Setiap personel yang menemukan atau mencurigai adanya indikasi kegagalan perlindungan Data Pribadi (seperti serangan siber, kehilangan laptop kerja, salah kirim data) wajib melaporkan kejadian tersebut kepada tim keamanan informasi/satuan kerja penanggung jawab siber dalam waktu kurang dari 1 jam sejak diketahui;

7.2. Tim teknis segera melakukan isolasi terhadap sistem yang terdampak (misalnya memutus koneksi jaringan server, menonaktifkan akun yang terkompromi) guna menghentikan kebocoran data lebih lanjut;

7.3. Pengendali Data Pribadi wajib memberikan notifikasi resmi secara tertulis mengenai insiden kebocoran kepada Lembaga Otoritas Pelindungan Data Pribadi dan Subjek Data Pribadi yang terdampak dalam waktu maksimal 3 x 24 jam sejak insiden diketahui.

**8. Pemusnahan Data yang Akuntabel**

8.1. Data pribadi yang telah habis masa retensinya, telah ditarik persetujuannya oleh pemiliknya, atau tidak lagi relevan dengan tujuan awal wajib dihapus atau dimusnahkan;

8.2. Proses pemusnahan secara digital wajib menggunakan metode penghapusan permanen yang tidak dapat dikembalikan (*sanitization/secure wiping*), sedangkan dokumen fisik wajib dihancurkan menggunakan mesin penghancur kertas (*shredder*) secara total untuk menjamin data tidak dapat direkonstruksi kembali;

8.3. Setiap aktivitas pemusnahan (baik fisik maupun digital) wajib dituangkan dalam Berita Acara Pemusnahan Data yang ditandatangani oleh petugas pelaksana dan saksi dari fungsi keamanan informasi.

Pj. SEKRETARIS DAERAH
KABUPATEN KENDAL,

AGUS DWI LESTARI