



PERATURAN MENTERI KOMUNIKASI DAN DIGITAL
REPUBLIK INDONESIA
NOMOR 5 TAHUN 2025
TENTANG
PENYELENGGARA SISTEM ELEKTRONIK LINGKUP PUBLIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KOMUNIKASI DAN DIGITAL REPUBLIK INDONESIA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 5 ayat (3), Pasal 6 ayat (4), Pasal 20 ayat (7), Pasal 81 ayat (4), Pasal 89, Pasal 97 ayat (5), dan Pasal 98 ayat (4) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik serta untuk memenuhi kebutuhan pengaturan dalam penyelenggaraan sistem elektronik lingkup publik, perlu menetapkan Peraturan Menteri Komunikasi dan Digital tentang Penyelenggara Sistem Elektronik Lingkup Publik;

Mengingat : 1. Pasal 17 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
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 beberapa kali diubah 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);
3. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916) sebagaimana telah diubah dengan Undang-Undang Nomor 61 Tahun 2024 tentang Perubahan atas Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 225, Tambahan Lembaran Negara Republik Indonesia

- Nomor 6994);
4. 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 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);
 5. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
 6. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
 7. Peraturan Presiden Nomor 174 Tahun 2024 tentang Kementerian Komunikasi dan Digital (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 370);
 8. Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2025 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Digital (Berita Negara Republik Indonesia Tahun 2025 Nomor 7);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI KOMUNIKASI DAN DIGITAL TENTANG PENYELENGGARA SISTEM ELEKTRONIK LINGKUP PUBLIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Penyelenggara Sistem Elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.
2. Penyelenggara Sistem Elektronik Lingkup Publik yang selanjutnya disebut PSE Lingkup Publik adalah Penyelenggaraan Sistem Elektronik oleh Instansi Penyelenggara Negara atau Institusi yang ditunjuk oleh Instansi Penyelenggara Negara.
3. PSE Lingkup Publik User Generated Content adalah PSE Lingkup Publik yang penyediaan, penayangan, pengunggahan, dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektroniknya dilakukan oleh Pengguna Sistem Elektronik.

4. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
5. Informasi Elektronik adalah satu atau sekumpulan Data Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
6. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
7. Data Elektronik adalah data berbentuk elektronik yang tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau perforasi.
8. 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.
9. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.
10. Klasifikasi Data Sesuai Risiko adalah proses untuk menentukan kelompok data dari semua jenis Data Elektronik yang dimiliki oleh PSE Lingkup Publik sesuai risiko yang ditimbulkan.
11. Data Terklasifikasi adalah kelompok Data Elektronik yang sudah diklasifikasi sesuai dengan tingkat risiko.
12. Arsip adalah rekaman kegiatan atau peristiwa dalam berbagai bentuk dan media sesuai dengan perkembangan teknologi informasi dan komunikasi yang dibuat dan diterima oleh lembaga negara, pemerintahan daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan, dan perseorangan dalam pelaksanaan kehidupan bermasyarakat, berbangsa, dan bernegara.

13. Reklasifikasi Data adalah penilaian ulang tingkat risiko atas Data Terklasifikasi yang telah ditetapkan berdasarkan Peninjauan Kembali.
14. Peninjauan Kembali adalah proses peninjauan terhadap kelompok Data Terklasifikasi secara periodik atau sewaktu-waktu sesuai kebutuhan.
15. Komputasi Awan adalah model penyediaan akses jaringan yang merata, mudah, berdasarkan permintaan untuk sekumpulan sumber daya komputasi yang dapat dikonfigurasi bersama antara lain jaringan, server, penyimpanan, aplikasi, dan layanan yang dapat disediakan dan dirilis dengan cepat dan dengan daya manajemen atau interaksi penyediaan pelayanan minimal.
16. Nama Domain adalah alamat internet penyelenggara negara, orang, badan usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
17. Nama Domain Instansi adalah alamat internet dari Instansi yang dapat digunakan dalam berkomunikasi melalui internet, berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
18. Registri Nama Domain adalah penyelenggara yang bertanggung jawab dalam melakukan pengelolaan, pengoperasian, dan pemeliharaan penyelenggaraan Sistem Elektronik Nama Domain.
19. Pejabat Nama Domain adalah pejabat yang ditunjuk dan ditetapkan oleh Pejabat Instansi untuk melakukan pendaftaran dan pengelolaan Nama Domain Instansi.
20. Pusat Data adalah fasilitas yang digunakan untuk penempatan Sistem Elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
21. Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.
22. Pemutusan Akses adalah tindakan pemblokiran Akses, penutupan akun dan/atau penghapusan konten.
23. Normalisasi adalah proses pemulihan Akses terhadap Sistem Elektronik yang telah ditutup agar dapat diakses kembali.
24. Kementerian atau Lembaga adalah Instansi Penyelenggara Negara yang bertugas mengawasi dan mengeluarkan pengaturan terhadap sektornya.
25. Instansi Penyelenggara Negara yang selanjutnya disebut Instansi adalah institusi legislatif, eksekutif, dan yudikatif di tingkat pusat dan daerah dan instansi lain yang dibentuk dengan peraturan perundang-undangan.

26. Instansi Pusat adalah kementerian, lembaga pemerintah nonkementerian, kesekretariatan lembaga negara, kesekretariatan lembaga nonstruktural, dan lembaga pemerintah lainnya.
27. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
28. Institusi yang ditunjuk oleh Instansi yang selanjutnya disebut Institusi adalah institusi yang melaksanakan penyelenggaraan Sistem Elektronik lingkup publik atas nama Instansi yang menunjuk.
29. Pemerintah Desa adalah kepala desa atau yang disebut dengan nama lain dibantu perangkat desa sebagai unsur penyelenggara pemerintah daerah.
30. Pejabat Instansi adalah pejabat pimpinan tinggi madya di Instansi Pusat, pejabat pimpinan tinggi madya di Pemerintah Daerah provinsi, pejabat pimpinan tinggi pratama di Pemerintah Daerah kabupaten/kota, pimpinan satuan organisasi unsur pembantu pemimpin atau unsur pimpinan.
31. Pembina Data adalah Instansi Pusat yang diberi kewenangan melakukan pembinaan terkait data atau instansi daerah yang diberikan penugasan untuk melakukan pembinaan terkait data sebagaimana diatur sesuai dengan ketentuan peraturan perundang-undangan bidang satu data Indonesia.
32. Produsen Data adalah unit pada Instansi yang menghasilkan data berdasarkan kewenangan sesuai dengan ketentuan peraturan perundang-undangan.
33. Walidata adalah unit pada Instansi yang melaksanakan kegiatan pengumpulan, pemeriksaan, dan pengelolaan Data yang disampaikan oleh Produsen Data, serta menyebarluaskan data.
34. Pengguna Sistem Elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang memanfaatkan barang, jasa, fasilitas, atau informasi yang disediakan oleh Penyelenggara Sistem Elektronik.
35. Forum Satu Data Indonesia adalah wadah komunikasi dan koordinasi Instansi Pusat dan/atau instansi daerah untuk penyelenggaraan satu data Indonesia.
36. Penyelenggara Jasa Akses Internet (Internet Service Provider) yang selanjutnya disingkat ISP adalah penyelenggara jasa multimedia yang menyelenggarakan jasa layanan akses internet untuk terhubung dengan jaringan internet publik.
37. Penyedia adalah pelaku usaha yang menyediakan barang/jasa berdasarkan kontrak.
38. Kementerian Komunikasi dan Digital yang selanjutnya disebut Kementerian adalah kementerian yang menyelenggarakan urusan pemerintahan di bidang

komunikasi dan informasi.

39. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi.
40. Direktur Jenderal adalah direktur jenderal yang tugas dan fungsinya di bidang penyelenggaraan sistem elektronik lingkup publik.

Pasal 2

Ruang lingkup Peraturan Menteri ini meliputi:

- a. pendaftaran Penyelenggara Sistem Elektronik Lingkup Publik;
- b. tata kelola dan moderasi Informasi Elektronik dan/atau Dokumen Elektronik;
- c. Pemutusan Akses Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang;
- d. penyelenggaraan Nama Domain Instansi;
- e. Klasifikasi Data Sesuai Risiko Penyelenggara Sistem Elektronik Lingkup Publik; dan
- f. pembinaan dan pengawasan.

Pasal 3

- (1) PSE Lingkup Publik meliputi:
 - a. Instansi; dan
 - b. Institusi.
- (2) PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) tidak termasuk PSE Lingkup Publik yang merupakan otoritas pengatur dan pengawas sektor keuangan.
- (3) Institusi sebagaimana dimaksud pada ayat (1) huruf b paling sedikit harus memenuhi kriteria:
 - a. memiliki tanda daftar Penyelenggara Sistem Elektronik Lingkup Privat sesuai peraturan perundang-undangan;
 - b. berbentuk badan hukum Indonesia; dan
 - c. memiliki pusat data yang berlokasi di wilayah Negara Kesatuan Republik Indonesia.
- (4) Penunjukan Institusi sebagaimana dimaksud pada ayat (1) huruf b merupakan penugasan yang ditetapkan dengan peraturan perundang-undangan.

BAB II

PENDAFTARAN PENYELENGGARA SISTEM ELEKTRONIK LINGKUP PUBLIK

Bagian Kesatu Umum

Pasal 4

- (1) Setiap PSE Lingkup Publik wajib melakukan pendaftaran PSE Lingkup Publik terhadap Sistem Elektronik yang diselenggarakannya.
- (2) Kewajiban pendaftaran PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) dilakukan sebelum Sistem Elektronik mulai digunakan oleh

Pengguna Sistem Elektronik.

- (3) Selain kewajiban melakukan pendaftaran sebagaimana dimaksud pada ayat (1), PSE Lingkup Publik wajib:
 - a. menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian;
 - b. melakukan perlindungan Data Pribadi; dan
 - c. melakukan uji kelaikan Sistem Elektronik, sesuai dengan ketentuan peraturan perundang-undangan.
- (4) Pendaftaran PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) diajukan kepada Menteri melalui layanan pendaftaran secara elektronik.

Pasal 5

- (1) PSE Lingkup Publik harus menunjuk pejabat pendaftar PSE Lingkup Publik.
- (2) Pejabat pendaftar PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) merupakan pejabat pendaftar yang berasal dari:
 - a. Instansi; atau
 - b. Institusi.

Pasal 6

- (1) Pejabat pendaftar PSE Lingkup Publik yang berasal dari Instansi sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a merupakan aparatur sipil negara yang menduduki paling rendah:
 - a. jabatan administrator pada satuan kerja atau perangkat daerah yang membidangi urusan komunikasi dan informatika; atau
 - b. jabatan fungsional ahli madya yang memiliki kompetensi bidang teknologi informasi dan komunikasi di satuan kerja atau perangkat daerah yang membidangi urusan komunikasi dan informatika.
- (2) Pejabat pendaftar PSE Lingkup Publik yang berasal dari Instansi sebagaimana dimaksud pada ayat (1) ditugaskan dengan surat tugas yang ditandatangani Pejabat Instansi.

Pasal 7

- (1) Pejabat pendaftar PSE Lingkup Publik yang berasal dari Institusi sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b merupakan pegawai dengan perjanjian kerja waktu tidak tertentu yang memimpin unit teknologi informasi dan komunikasi di Institusi.
- (2) Pejabat pendaftar PSE Lingkup Publik yang berasal dari Institusi sebagaimana dimaksud pada ayat (1) ditugaskan dengan surat tugas yang ditandatangani pimpinan Institusi.

Pasal 8

- (1) Pejabat pendaftar PSE Lingkup Publik sebagaimana dimaksud dalam Pasal 5 melaksanakan pendaftaran PSE Lingkup Publik sebagaimana dimaksud dalam Pasal 4 ayat (1).
- (2) Dalam melaksanakan pendaftaran Lingkup Publik sebagaimana dimaksud pada ayat (1), pejabat pendaftar PSE Lingkup Publik harus:
 - a. memastikan kebenaran dan keakuratan seluruh data pendaftaran PSE Lingkup Publik;
 - b. melakukan pembaruan data pendaftaran PSE Lingkup Publik sesuai dengan kondisi terkini dari Sistem Elektronik;
 - c. menjaga kerahasiaan Akses yang terdiri atas identitas pengguna dan kata sandi, serta data pendaftaran PSE Lingkup Publik;
 - d. mengisi informasi pelaksanaan prosedur dan sistem, serta ketersediaan sarana pengamanan dalam penyelenggaraan Sistem Elektronik; dan
 - e. melaporkan hasil kegiatan pendaftaran PSE Lingkup Publik kepada Pejabat Instansi atau pimpinan Institusi.

Pasal 9

- (1) Pejabat pendaftar PSE Lingkup Publik harus membuktikan penugasan untuk melaksanakan pendaftaran PSE Lingkup Publik dengan mengunggah surat tugas melalui layanan pendaftaran secara elektronik.
- (2) Selain mengunggah surat tugas sebagaimana dimaksud pada ayat (1) Pejabat pendaftar PSE Lingkup Publik harus memberikan informasi pejabat pendaftar PSE Lingkup Publik mengenai:
 - a. jenis Instansi atau Institusi;
 - b. nama Instansi atau Institusi;
 - c. nama unit kerja;
 - d. nomor telepon unit kerja;
 - e. status pejabat pendaftar PSE Lingkup Publik;
 - f. nama lengkap pejabat pendaftar PSE Lingkup Publik;
 - g. nomor induk pegawai pejabat pendaftar PSE Lingkup Publik untuk Instansi, atau nomor pegawai pejabat pendaftar untuk Institusi.
 - h. nama jabatan pejabat pendaftar PSE Lingkup Publik;
 - i. nomor telepon seluler pejabat pendaftar PSE Lingkup Publik; dan
 - j. alamat surat elektronik (*email*) resmi Instansi sebagai PSE Lingkup Publik.
- (3) Informasi sebagaimana dimaksud pada ayat (2) dapat memanfaatkan sistem aplikasi pelayanan kepegawaian.
- (4) Dalam hal pengisian informasi mengenai pejabat

pendaftar PSE Lingkup Publik sebagaimana dimaksud pada ayat (2), pejabat pendaftar PSE Lingkup Publik yang berasal dari Institusi harus melampirkan dasar penunjukan Institusi sebagaimana dimaksud dalam Pasal 3 ayat (4).

- (5) Kementerian melakukan verifikasi terhadap informasi mengenai pejabat pendaftar PSE Lingkup Publik sebagaimana dimaksud pada ayat (2) dan ayat (4).

Pasal 10

- (1) Dalam hal terjadi pergantian pejabat pendaftar PSE Lingkup Publik sebagaimana dimaksud dalam Pasal 9 ayat (1) PSE Lingkup Publik harus menugaskan pejabat yang menggantikan pejabat pendaftar PSE Lingkup Publik.
- (2) Pejabat yang menggantikan pejabat pendaftar PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) harus:
 - a. mengunggah surat tugas sebagaimana dimaksud dalam Pasal 9 ayat (1); dan
 - b. mengisi informasi sebagaimana dimaksud dalam Pasal 9 ayat (2) dan ayat (4).
- (3) Kementerian melakukan verifikasi terhadap informasi mengenai pejabat yang menggantikan pejabat pendaftar PSE Lingkup Publik sebagaimana dimaksud pada ayat (2).

Bagian Kedua

Pendaftaran Sistem Elektronik yang Dikelola PSE Lingkup Publik

Pasal 11

- (1) Pendaftaran Sistem Elektronik yang dikelola PSE Lingkup Publik harus dilakukan oleh pejabat pendaftar PSE Lingkup Publik.
- (2) PSE Lingkup Publik melalui pejabat pendaftar PSE Lingkup Publik memberikan informasi yang benar dalam pengisian formulir pendaftaran Sistem Elektronik yang dikelola PSE Lingkup Publik mengenai:
 - a. gambaran umum pengoperasian Sistem Elektronik;
 - b. pemenuhan kewajiban untuk memastikan keamanan informasi sesuai dengan ketentuan peraturan perundang-undangan;
 - c. pemenuhan kewajiban untuk menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian sesuai dengan ketentuan peraturan perundang-undangan;
 - d. pemenuhan kewajiban melakukan perlindungan Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;
 - e. pemenuhan kewajiban melakukan uji kelaikan

- Sistem Elektronik sesuai dengan ketentuan peraturan perundang-undangan; dan
- f. pemenuhan ketentuan arsitektur sistem pemerintahan berbasis elektronik nasional dan arsitektur sistem pemerintahan berbasis elektronik Instansi Pusat dan Pemerintah Daerah sesuai dengan ketentuan peraturan perundang-undangan dalam penyelenggaraan sistem elektronik.
- (3) Kementerian melakukan pengecekan kelengkapan terhadap isian formulir pendaftaran Sistem Elektronik yang dikelola PSE Lingkup Publik.
 - (4) Dalam hal informasi sebagaimana dimaksud pada ayat (2) telah disampaikan dengan lengkap berdasarkan pengecekan sebagaimana dimaksud pada ayat (3), Kementerian dapat menyetujui pendaftaran atas Sistem Elektronik yang dikelola PSE Lingkup Publik.
 - (5) Persetujuan pendaftaran sebagaimana dimaksud pada ayat (4) merupakan persetujuan atas kelengkapan dokumen dan informasi yang diajukan oleh Instansi sebagaimana dimaksud pada ayat (2).

Pasal 12

Pejabat pendaftar PSE Lingkup Publik mengisi informasi mengenai gambaran umum pengoperasian Sistem Elektronik sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a, yang terdiri atas:

- a. nama Sistem Elektronik;
- b. pemilik Sistem Elektronik;
- c. bidang/sektor Sistem Elektronik;
- d. informasi mengenai narahubung Sistem Elektronik;
- e. *uniform resource locator* (URL) situs web;
- f. sistem Nama Domain (*domain name system*) dan/atau alamat *internet protocol* (IP) *server*;
- g. deskripsi singkat fungsi Sistem Elektronik dan proses bisnis Sistem Elektronik;
- h. kategori Sistem Elektronik berdasarkan asas risiko;
- i. Data Terklasifikasi yang dikelola;
- j. keterangan Data Pribadi yang diproses; dan
- k. keterangan lokasi pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik.

Bagian Ketiga

Penerbitan Tanda Daftar PSE Lingkup Publik

Pasal 13

- (1) Menteri menerbitkan tanda daftar PSE Lingkup Publik dalam hal pendaftaran atas Sistem Elektronik yang dikelola PSE Lingkup Publik disetujui sebagaimana dimaksud dalam Pasal 11 ayat (4).
- (2) Tanda daftar PSE Lingkup Publik pada ayat (1) ditempatkan dalam daftar PSE Lingkup Publik yang dimuat di laman situs web yang dikelola oleh Kementerian.

- (3) Tanda daftar PSE Lingkup Publik sebagaimana dimaksud pada ayat (2) memuat informasi paling sedikit:
 - a. logo Kementerian;
 - b. nama PSE Lingkup Publik;
 - c. nomor tanda daftar PSE Lingkup Publik;
 - d. nama pejabat pendaftar PSE Lingkup Publik;
 - e. nama Sistem Elektronik;
 - f. fungsi Sistem Elektronik;
 - g. versi Sistem Elektronik;
 - h. tanggal terbit;
 - i. *barcode* tanda daftar PSE Lingkup Publik; dan
 - j. nama dan tanda tangan pejabat penandatanganan tanda daftar PSE Lingkup Publik.
- (4) Pejabat pendaftar PSE Lingkup Publik dapat mengunduh tanda daftar PSE Lingkup Publik yang telah terbit melalui layanan elektronik yang diselenggarakan oleh Kementerian.
- (5) PSE Lingkup Publik yang telah mendapatkan tanda daftar PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) harus mencantumkan tanda daftar tersebut pada setiap Sistem Elektronik yang telah didaftarkan.
- (6) Tanda daftar PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) merupakan persyaratan pengajuan permohonan rekomendasi belanja (*clearance*) pengembangan Sistem Elektronik di Instansi.

Bagian Keempat
Pembaruan Tanda Daftar PSE Lingkup Publik

Pasal 14

- (1) Dalam hal informasi pendaftaran Sistem Elektronik yang dikelola PSE Lingkup Publik sebagaimana dimaksud dalam Pasal 11 ayat (2) mengalami perubahan, PSE Lingkup Publik melalui pejabat pendaftar PSE Lingkup Publik wajib melakukan pembaruan isian formulir pendaftaran Sistem Elektronik yang dikelola PSE Lingkup Publik.
- (2) Kementerian melakukan pengecekan kelengkapan terhadap pembaruan isian formulir pendaftaran Sistem Elektronik yang dikelola PSE Lingkup Publik sebagaimana dimaksud pada ayat (1).
- (3) Dalam hal berdasarkan pengecekan sebagaimana dimaksud pada ayat (2) pembaruan isian formulir pendaftaran Sistem Elektronik dinyatakan lengkap, Menteri memperbarui tanda daftar PSE Lingkup Publik.

Bagian Kelima
Penghapusan Tanda Daftar PSE Lingkup Publik

Pasal 15

- (1) Dalam hal Sistem Elektronik sudah tidak digunakan, pejabat pendaftar PSE Lingkup Publik harus menyampaikan surat keterangan yang menyatakan Sistem Elektronik sudah tidak digunakan melalui layanan elektronik yang diselenggarakan oleh Kementerian.
- (2) Surat keterangan sebagaimana dimaksud pada ayat (1) ditandatangani oleh Pejabat Instansi.
- (3) Menteri melakukan penghapusan tanda daftar PSE Lingkup Publik setelah menerima surat keterangan sebagaimana dimaksud pada ayat (2).

Bagian Keenam
Sanksi Administratif dan Normalisasi

Pasal 16

- (1) Menteri mengenakan sanksi administratif kepada PSE Lingkup Publik yang:
 - a. tidak melakukan pendaftaran PSE Lingkup Publik sebagaimana dimaksud dalam Pasal 4 ayat (1);
 - b. tidak memenuhi kewajiban sebagaimana dimaksud dalam Pasal 4 ayat (3); dan/atau
 - c. telah mempunyai tanda daftar tetapi tidak melaporkan perubahan informasi pendaftaran Sistem Elektronik yang dikelola PSE Lingkup Publik sebagaimana dimaksud dalam Pasal 14 ayat (1).
- (2) Pengenaan sanksi administratif sebagaimana dimaksud pada ayat (1) dilakukan melalui koordinasi dengan pimpinan Kementerian atau Lembaga terkait.
- (3) Dalam hal PSE Lingkup Publik tidak melakukan pendaftaran sebagaimana dimaksud pada ayat (1) huruf a, Menteri mengenakan sanksi administratif berupa Pemutusan Akses dalam bentuk pemblokiran terhadap Sistem Elektronik (*access blocking*).
- (4) Dalam hal PSE Lingkup Publik tidak memberikan informasi pendaftaran dengan benar sebagaimana dimaksud pada ayat (1) huruf b atau telah mempunyai tanda daftar tetapi tidak melaporkan perubahan terhadap informasi pendaftaran sebagaimana dimaksud pada ayat (1) huruf c, Menteri mengenakan sanksi administratif berupa:
 - a. teguran tertulis yang disampaikan melalui surat elektronik (*electronic mail*) dan/atau media elektronik lainnya yang diberikan kepada PSE Lingkup Publik sebanyak 3 (tiga) kali untuk setiap 7 x 24 (tujuh kali dua puluh empat) jam;
 - b. penghentian sementara terhadap PSE Lingkup

Publik dalam hal tidak mengindahkan teguran tertulis dalam jangka waktu 7 (tujuh) hari sejak teguran ketiga dikirimkan sebagaimana dimaksud dalam huruf a; dan/atau

- c. Pemutusan Akses dalam bentuk pemblokiran terhadap Sistem Elektronik (*access blocking*) dan dikeluarkan dari daftar PSE Lingkup Publik dalam hal PSE Lingkup Publik tidak memberikan konfirmasi dalam jangka waktu 7 (tujuh) hari setelah penghentian sementara sebagaimana dimaksud dalam huruf b.

Pasal 17

- (1) Dalam hal PSE Lingkup Publik telah memenuhi ketentuan pendaftaran sebagaimana dimaksud dalam Pasal 5 sampai dengan Pasal 12, Menteri melakukan Normalisasi terhadap Sistem Elektronik yang diputus aksesnya (*access blocking*) sebagaimana dimaksud dalam Pasal 16 ayat (3).
- (2) Dalam hal PSE Lingkup Publik telah melakukan pembaruan informasi pendaftaran dengan benar, Menteri melakukan Normalisasi terhadap Sistem Elektronik yang dihentikan sementara sebagaimana dimaksud dalam Pasal 16 ayat (4) huruf b.
- (3) Dalam hal PSE Lingkup Publik telah melakukan pendaftaran ulang dengan memberikan informasi pendaftaran dengan benar, Menteri melakukan Normalisasi terhadap Sistem Elektronik yang diputus aksesnya dan dikeluarkan dari daftar PSE Lingkup Publik sebagaimana dimaksud dalam Pasal 16 ayat (4) huruf c.
- (4) Normalisasi sebagaimana dimaksud pada ayat (1), ayat (2) dan ayat (3) dilakukan melalui tahapan:
 - a. PSE Lingkup Publik melalui Pejabat Instansi atau pimpinan Institusi mengajukan permohonan Normalisasi kepada Menteri; dan
 - b. Permohonan Normalisasi sebagaimana dimaksud dalam huruf a diajukan dengan melampirkan:
 1. surat permohonan tertulis; dan
 2. tanda daftar PSE Lingkup Publik.

BAB III

TATA KELOLA DAN MODERASI INFORMASI ELEKTRONIK DAN/ATAU DOKUMEN ELEKTRONIK

Bagian Kesatu Umum

Pasal 18

- (1) PSE Lingkup Publik harus menyelenggarakan Sistem Elektronik dan mengelola Informasi Elektronik dan/atau Dokumen Elektronik di dalam Sistem Elektronik secara andal, aman, dan bertanggung jawab.

- (2) PSE Lingkup Publik harus menyediakan petunjuk penggunaan layanan dalam bahasa Indonesia sesuai dengan ketentuan peraturan perundang-undangan.
- (3) PSE Lingkup Publik wajib memastikan Sistem Elektroniknya:
 - a. tidak memuat; dan
 - b. tidak memfasilitasi penyebaran, Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.
- (4) Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud pada ayat (3) merupakan Informasi Elektronik dan/atau Dokumen Elektronik dengan klasifikasi:
 - a. melanggar ketentuan peraturan perundang-undangan;
 - b. meresahkan masyarakat dan mengganggu ketertiban umum; dan
 - c. memberitahukan cara atau menyediakan Akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.
- (5) Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud pada ayat (4) bersifat mendesak jika memuat:
 - a. terorisme;
 - b. pornografi anak; atau
 - c. konten yang meresahkan masyarakat dan mengganggu ketertiban umum.
- (6) Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud pada ayat (4) huruf b ditetapkan oleh Kementerian atau Lembaga sesuai dengan ketentuan peraturan perundang-undangan.
- (7) PSE Lingkup Publik yang tidak melakukan kewajiban sebagaimana dimaksud pada ayat (3) diputus Akses terhadap Sistem Elektroniknya (*access blocking*).

Bagian Kedua
Kewajiban PSE Lingkup Publik
User Generated Content

Pasal 19

- (1) Dalam rangka memenuhi kewajiban sebagaimana dimaksud dalam Pasal 18 ayat (3), PSE Lingkup Publik *User Generated Content* wajib:
 - a. memiliki tata kelola mengenai Informasi Elektronik dan/atau Dokumen Elektronik; dan
 - b. menyediakan sarana pelaporan.
- (2) Tata kelola sebagaimana dimaksud pada ayat (1) huruf a paling sedikit memuat ketentuan:
 - a. kewajiban dan hak Pengguna Sistem Elektronik dalam menggunakan layanan Sistem Elektronik;
 - b. kewajiban dan hak PSE Lingkup Publik dalam melaksanakan operasional Sistem Elektronik;

- c. pertanggungjawaban terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang diunggah Pengguna Sistem Elektronik; dan
 - d. ketersediaan sarana dan layanan serta penyelesaian pengaduan.
- (3) Sarana pelaporan sebagaimana dimaksud pada ayat (1) huruf b harus mampu diakses oleh publik dan digunakan untuk penyampaian aduan dan/atau laporan atas Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang yang termuat pada Sistem Elektronik yang dikelolanya.
- (4) Terhadap aduan dan/atau laporan atas Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud pada ayat (3), PSE Lingkup Publik *User Generated Content* wajib:
- a. memberikan tanggapan terhadap aduan dan/atau laporan kepada pihak yang mengadukan dan/atau pihak yang melaporkan;
 - b. melakukan pemeriksaan secara mandiri atas aduan dan/atau laporan dan/atau meminta verifikasi aduan dan/atau laporan kepada Menteri dan/atau Kementerian atau Lembaga terkait;
 - c. memberikan pemberitahuan kepada Pengguna Sistem Elektronik mengenai aduan dan/atau laporan terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang diunggah oleh Pengguna Sistem Elektronik; dan
 - d. menolak aduan dan/atau laporan apabila Informasi Elektronik dan/atau Dokumen Elektronik yang dilaporkan bukan merupakan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.
- (5) PSE Lingkup Publik *User Generated Content* yang tidak melakukan kewajiban sebagaimana dimaksud pada ayat (1) dan ayat (4) diputus Akses terhadap Sistem Elektroniknya (*access blocking*).

Pasal 20

- (1) PSE Lingkup Publik *User Generated Content* dapat dibebaskan dari tanggung jawab hukum mengenai Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 18 ayat (4) yang ditransmisikan atau didistribusikan melalui Sistem Elektroniknya dalam hal PSE Lingkup Publik *User Generated Content*:
- a. telah melakukan kewajiban sebagaimana dimaksud dalam Pasal 18 ayat (3) dan Pasal 19;
 - b. memberikan informasi Pengguna Sistem Elektronik yang mengunggah Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang dalam rangka pengawasan dan/atau penegakan hukum; dan
 - c. melakukan Pemutusan Akses dalam bentuk penghapusan konten (*take down*) terhadap

Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.

- (2) Informasi Pengguna Sistem Elektronik sebagaimana dimaksud pada ayat (1) huruf b merupakan Data Elektronik yang dikontrol atau dikelola oleh PSE Lingkup Publik *User Generated Content* terkait dengan layanan yang digunakan oleh Pengguna Sistem Elektronik meliputi:
 - a. informasi mengenai identitas Pengguna Sistem Elektronik, termasuk nama Pengguna Sistem Elektronik yang digunakan dalam layanan pada PSE Lingkup Publik *User Generated Content*;
 - b. alamat tempat tinggal Pengguna Sistem Elektronik dan alamat lain yang mengidentifikasi lokasi Pengguna Sistem Elektronik pada waktu mendaftar atau menggunakan layanan PSE Lingkup Publik *User Generated Content*;
 - c. nomor identifikasi yang digunakan oleh Pengguna Sistem Elektronik untuk mendaftar layanan pada PSE Lingkup Publik *User Generated Content*; dan
 - d. informasi pembayaran atau tagihan yang dikeluarkan oleh PSE Lingkup Publik *User Generated Content* kepada Pengguna Sistem Elektronik terkait lokasi instalasi peralatan dan durasi layanan.

BAB IV PEMUTUSAN AKSES INFORMASI ELEKTRONIK DAN/ATAU DOKUMEN ELEKTRONIK YANG DILARANG

Bagian Kesatu Umum

Pasal 21

- (1) Menteri berwenang melakukan:
 - a. Pemutusan Akses; dan
 - b. memerintahkan pada PSE Publik untuk melakukan pemutusan Akses, terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 18 ayat (4).
- (2) Selain kewenangan dimaksud sebagaimana pada ayat (1), Menteri berwenang melakukan Normalisasi.
- (3) Menteri menugaskan Direktur Jenderal dalam melaksanakan kewenangan sebagaimana dimaksud pada ayat (1) dan ayat (2).

Pasal 22

PSE Lingkup Publik wajib melakukan Pemutusan Akses dalam bentuk penghapusan konten (*take down*) terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 18 ayat (4)

berdasarkan perintah Menteri.

Pasal 23

- (1) Permohonan Pemutusan Akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 18 dapat diajukan oleh:
 - a. masyarakat;
 - b. Kementerian atau Lembaga;
 - c. aparat penegak hukum; dan/atau
 - d. lembaga peradilan.
- (2) Permohonan sebagaimana dimaksud pada ayat (1) dapat disampaikan melalui:
 - a. situs web (*website*) dan/atau aplikasi;
 - b. surat non elektronik; dan/atau
 - c. surat elektronik (*electronic mail*).

Bagian Kedua

Permohonan Pemutusan Akses oleh Masyarakat

Pasal 24

- (1) Permohonan oleh masyarakat terkait Pemutusan Akses Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 23 ayat (1) huruf a disampaikan kepada:
 - a. Kementerian atau Lembaga yang berwenang untuk permohonan Pemutusan Akses terhadap:
 1. Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang yang berada di bawah kewenangannya; dan/atau
 2. Informasi Elektronik dan/atau Dokumen Elektronik yang dapat memfasilitasi diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang yang berada di bawah kewenangannya, berdasarkan ketentuan peraturan perundang-undangan; atau
 - b. Direktur Jenderal untuk permohonan Pemutusan Akses terhadap:
 1. Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang yang bermuatan pornografi dan/atau perjudian; dan/atau
 2. Informasi Elektronik dan/atau Dokumen Elektronik yang dapat memfasilitasi diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang yang bermuatan pornografi dan/atau perjudian.
- (2) Permohonan Pemutusan Akses yang diajukan oleh masyarakat sebagaimana dimaksud pada ayat (1) disampaikan secara tertulis dan paling sedikit memuat informasi:
 - a. identitas pemohon;
 - b. gambar atau tangkapan layar (*screen capture*) yang

- menampilkan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang;
 - c. tautan atau *Uniform Resource Locator (URL)* yang spesifik mengarah ke Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang yang dimohonkan untuk diputus aksesnya; dan
 - d. alasan yang menjadi dasar permohonan.
- (3) Kementerian atau Lembaga yang menerima permohonan Pemutusan Akses dari masyarakat sebagaimana dimaksud pada ayat (1) huruf a mengajukan permohonan Pemutusan Akses kepada Direktur Jenderal.

Bagian Ketiga

Pengajuan Pemutusan Akses oleh Kementerian atau Lembaga, Aparat Penegak Hukum dan Lembaga Peradilan

Pasal 25

- (1) Kementerian atau Lembaga terkait berkoordinasi dengan Direktur Jenderal untuk Pemutusan Akses Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 18 ayat (4).
- (2) Aparat penegak hukum dapat meminta Pemutusan Akses Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 18 ayat (4) kepada Direktur Jenderal.
- (3) Lembaga peradilan dapat memerintahkan Pemutusan Akses Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud dalam Pasal 18 ayat (4) kepada Direktur Jenderal.
- (4) Pemutusan Akses sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) diajukan oleh Kementerian atau Lembaga, aparat penegak hukum, atau Lembaga Peradilan secara tertulis dan paling sedikit melampirkan:
 - a. surat resmi dari Kementerian atau Lembaga, aparat penegak hukum, atau surat penetapan dan/atau putusan pengadilan dari lembaga peradilan;
 - b. analisis hukum mengenai Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang;
 - c. gambar atau tangkapan layar (*screen capture*) yang menampilkan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang; dan
 - d. tautan atau *Uniform Resource Locator (URL)* yang spesifik mengarah ke Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.
- (5) Pengajuan Pemutusan Akses secara tertulis dari Kementerian atau Lembaga, aparat penegak hukum, dan/atau lembaga peradilan dilakukan oleh narahubung sebagaimana dimaksud dalam Pasal 12 huruf d.
- (6) Dalam hal Kementerian atau Lembaga, aparat penegak

hukum, dan/atau lembaga peradilan tidak menunjuk narahubung sebagaimana dimaksud pada ayat (5), pengajuan Pemutusan Akses dilakukan oleh pejabat pendaftar PSE Lingkup Publik.

Bagian Keempat
Pelaksanaan Pemutusan Akses

Pasal 26

- (1) Direktur Jenderal memerintahkan PSE Lingkup Publik untuk melakukan Pemutusan Akses dalam bentuk penghapusan konten (*take down*) terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.
- (2) Perintah Pemutusan Akses dalam bentuk penghapusan konten (*take down*) sebagaimana dimaksud pada ayat (1) disampaikan melalui surat elektronik (*electronic mail*) atau Sistem Elektronik lainnya.
- (3) PSE Lingkup Publik yang diperintahkan melakukan Pemutusan Akses dalam bentuk penghapusan konten (*take down*) sebagaimana dimaksud pada ayat (1) wajib melakukan Pemutusan Akses (*take down*) terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang paling lambat 1 x 24 (satu kali dua puluh empat) jam setelah surat perintah Pemutusan Akses diterima.
- (4) Direktur Jenderal melakukan Pemutusan Akses dan/atau memerintahkan ISP untuk melakukan Pemutusan Akses terhadap Sistem Elektronik dalam bentuk pemblokiran (*access blocking*) dalam hal PSE Lingkup Publik tidak melaksanakan Pemutusan Akses dalam bentuk penghapusan konten (*take down*) terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sebagaimana dimaksud pada ayat (3).
- (5) Permohonan Pemutusan Akses dalam bentuk penghapusan konten (*take down*) terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang bersifat mendesak sebagaimana dimaksud dalam Pasal 18 ayat (5), PSE Lingkup Publik wajib melakukan Pemutusan Akses dalam bentuk penghapusan konten (*take down*) terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang sesegera mungkin tanpa penundaan paling lambat 4 (empat) jam setelah peringatan diterima.
- (6) Direktur Jenderal melakukan Pemutusan Akses dan/atau memerintahkan ISP untuk melakukan Pemutusan Akses dalam bentuk pemblokiran terhadap Sistem Elektronik (*access blocking*) yang diselenggarakan oleh PSE Lingkup Publik dalam hal PSE Lingkup Publik tidak melaksanakan Pemutusan Akses dalam bentuk penghapusan konten (*take down*) sebagaimana dimaksud pada ayat (4).

Bagian Kelima
Peran Penyelenggara Jasa Akses Internet
(*Internet Service Provider*)

Pasal 27

- (1) ISP wajib melakukan Pemutusan Akses dalam bentuk pemblokiran terhadap Sistem Elektronik PSE Lingkup Publik (*access blocking*) yang diperintahkan oleh Direktur Jenderal untuk diputus aksesnya sebagaimana dimaksud dalam Pasal 26 ayat (4) dan ayat (6).
- (2) Pemutusan Akses dalam bentuk pemblokiran (*access blocking*) sebagaimana dimaksud pada ayat (1) hanya dapat dilakukan oleh Direktur Jenderal.
- (3) Pemutusan Akses dalam bentuk pemblokiran (*access blocking*) oleh ISP sebagaimana dimaksud pada ayat (1) dan ayat (2) dilakukan dengan tata cara, metode, dan/atau teknologi yang ditetapkan oleh Direktur Jenderal.
- (4) ISP yang tidak melakukan Pemutusan Akses dalam bentuk pemblokiran (*access blocking*) sebagaimana dimaksud pada ayat (1) dikenai sanksi sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 28

- (1) ISP wajib menampilkan laman labuh (*landing page*) dalam melakukan Pemutusan Akses dalam bentuk pemblokiran terhadap Sistem Elektronik (*access blocking*) bermuatan Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang dan/atau memfasilitasi penyebaran Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.
- (2) Laman labuh (*landing page*) sebagaimana dimaksud pada ayat (1) tidak memuat Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang dan/atau menawarkan produk yang dilarang sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Keenam
Normalisasi

Pasal 29

- (1) Permohonan Normalisasi diajukan kepada Direktur Jenderal oleh:
 - a. PSE Lingkup Publik yang diputus akses terhadap Sistem Elektroniknya (*access blocking*); atau
 - b. Kementerian atau Lembaga.
- (2) Permohonan Normalisasi oleh PSE Lingkup Publik yang diputus akses terhadap Sistem Elektroniknya (*access blocking*) sebagaimana dimaksud pada ayat (1) huruf a diajukan dengan melampirkan:
 - a. surat permohonan tertulis;

- b. identitas penanggung jawab Sistem Elektronik dan nomor kontak yang dapat dihubungi;
 - c. hasil pindai kartu identitas pemilik dan/atau penanggung jawab Sistem Elektronik;
 - d. gambar atau tangkapan layar (*screen capture*) dan tautan atau *link (URL)* yang membuktikan bahwa Sistem Elektronik tidak lagi memuat Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang;
 - e. surat rekomendasi dari Kementerian atau Lembaga, aparat penegak hukum, atau putusan pengadilan yang berkekuatan hukum tetap; dan
 - f. bukti lainnya yang mendukung legitimasi sebagai PSE Lingkup Publik.
- (3) Penanggung jawab sebagaimana dimaksud pada ayat (2) huruf b merupakan:
- a. Pejabat Instansi; atau
 - b. pimpinan Institusi.
- (4) Permohonan Normalisasi oleh Kementerian atau Lembaga sebagaimana dimaksud pada ayat (1) huruf b diajukan melalui surat permohonan tertulis.
- (5) Direktur Jenderal menindaklanjuti permohonan Normalisasi yang memenuhi ketentuan sebagaimana dimaksud pada ayat (2) dan ayat (4) paling lama 2x24 (dua kali dua puluh empat) jam.
- (6) Direktur Jenderal berwenang menolak permohonan Normalisasi terhadap Sistem Elektronik yang telah diputus aksesnya (*access blocking*) lebih dari 3 (tiga) kali.

BAB V

PENYELENGGARAAN NAMA DOMAIN INSTANSI

Bagian Kesatu Umum

Pasal 30

Penyelenggaraan Nama Domain Instansi dalam Peraturan Menteri ini meliputi:

- a. penggunaan Nama Domain Instansi;
- b. pengelolaan Nama Domain Instansi;
- c. penggunaan *server* Nama Domain Instansi; dan
- d. penyelesaian perselisihan Nama Domain Instansi.

Bagian Kedua Penggunaan Nama Domain Instansi

Pasal 31

Instansi harus menggunakan Nama Domain Instansi dan bertanggung jawab atas penggunaan Nama Domain Instansi yang digunakan.

Pasal 32

- (1) Nama Domain Instansi terdiri atas:
 - a. Nama Domain tingkat kedua; dan
 - b. Nama Domain tingkat turunan.
- (2) Nama Domain tingkat kedua sebagaimana dimaksud pada ayat (1) huruf a terdiri atas:
 - a. Nama Domain .go.id;
 - b. Nama Domain .desa.id.; dan
 - c. Nama Domain lain terkait penyebutan lain dari desa sesuai dengan ketentuan peraturan perundang-undangan.
- (3) Nama Domain .go.id sebagaimana dimaksud pada ayat (2) huruf a digunakan untuk:
 - a. alamat elektronik resmi Instansi;
 - b. layanan administrasi pemerintahan nasional atau layanan publik nasional; dan/atau
 - c. kegiatan berskala nasional atau internasional.
- (4) Nama Domain .desa.id sebagaimana dimaksud pada ayat (2) huruf b digunakan untuk alamat elektronik resmi Pemerintah Desa.
- (5) Nama Domain lain terkait penyebutan lain dari desa sebagaimana dimaksud pada ayat (2) huruf c dan penggunaannya ditetapkan oleh Menteri.

Pasal 33

- (1) Instansi vertikal dari Instansi Pusat yang berada di daerah atau perwakilan di luar negeri, atau perangkat kewilayahan pada Pemerintah Daerah, dapat menggunakan Nama Domain Instansi sebagai alamat elektronik resmi Instansi.
- (2) Alamat elektronik resmi dari unit kerja pada Instansi menggunakan subdomain dari Nama Domain Instansi.
- (3) Instansi menetapkan kebijakan mengenai tata cara pengelolaan Nama Domain dan subdomain di lingkungan Instansi.

Pasal 34

- (1) Pemerintah Desa harus menggunakan Nama Domain sebagaimana dimaksud dalam pasal 32 ayat (4) untuk penyelenggaraan pemerintahan desa.
- (2) Alamat elektronik resmi dari unit kerja pada Pemerintah Desa menggunakan subdomain dari Nama Domain Pemerintah Desa.

Pasal 35

Penggunaan Nama Domain untuk kegiatan berskala nasional dan/atau internasional sebagaimana dimaksud dalam pasal 32 ayat (3) huruf c dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Ketiga
Pengelolaan Nama Domain Instansi

Pasal 36

- (1) Pengelolaan Nama Domain Instansi sebagaimana dimaksud dalam Pasal 30 huruf b meliputi:
 - a. pendaftaran Nama Domain Instansi;
 - b. perpanjangan Nama Domain Instansi;
 - c. penonaktifan dan penghapusan Nama Domain Instansi;
 - d. perubahan Nama Domain Instansi;
 - e. perubahan data Pejabat Nama Domain Instansi;
 - f. pengalihan Nama Domain Instansi;
 - g. pembatalan Nama Domain Instansi;
 - h. pemulihan Nama Domain Instansi;
 - i. penanganan keluhan Nama Domain Instansi; dan
 - j. pemantauan, evaluasi, dan pembiayaan.
- (2) Pengelolaan Nama Domain Instansi sebagaimana dimaksud pada ayat (1) dilakukan melalui layanan elektronik yang diselenggarakan oleh Kementerian.
- (3) Pengelolaan Nama Domain Instansi sebagaimana dimaksud pada ayat (1) dikecualikan untuk pengelolaan Nama Domain bagi kepentingan militer yang mengacu pada peraturan yang ditetapkan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang pertahanan dan keamanan.
- (4) Pengelolaan subdomain di lingkungan Instansi dilakukan oleh satuan kerja yang mengelola teknologi informasi dan komunikasi.

Pasal 37

- (1) Menteri merupakan registrar Nama Domain untuk Nama Domain Instansi sebagaimana dimaksud dalam Pasal 32 ayat (1).
- (2) Dalam melaksanakan registrar Nama Domain Instansi sebagaimana dimaksud pada ayat (1), Menteri dapat menugaskan Direktur Jenderal.

Paragraf 1

Pendaftaran Nama Domain Instansi

Pasal 38

- (1) Pejabat Instansi atas nama pimpinan Instansi mengajukan pendaftaran Nama Domain .go.id. sebagaimana dimaksud dalam Pasal 32 ayat (3) kepada Direktur Jenderal.
- (2) Format penulisan Nama Domain .go.id sebagaimana dimaksud pada ayat (1) harus terdiri atas:
 - a. karakter yang dapat berupa nama atau singkatan nama atau akronim dari nama resmi Instansi;
 - b. nama layanan administrasi pemerintahan nasional;
 - c. nama layanan publik nasional; dan/atau
 - d. nama kegiatan berskala nasional atau

internasional.

- (3) Pengajuan pendaftaran Nama Domain Instansi yang digunakan untuk alamat elektronik resmi Instansi sebagaimana dimaksud dalam Pasal 32 ayat (3) huruf a melampirkan:
 - a. surat permohonan Nama Domain Instansi;
 - b. dasar hukum yang menjadi ketentuan pembentukan Instansi;
 - c. surat penunjukan Pejabat Nama Domain; dan
 - d. kartu aparatur sipil negara, kartu anggota TNI, kartu anggota POLRI, atau kartu identitas pegawai tetap Pejabat Nama Domain.
- (4) Pengajuan pendaftaran Nama Domain Instansi yang digunakan untuk layanan administrasi pemerintahan nasional atau layanan publik nasional sebagaimana dimaksud dalam Pasal 32 ayat (3) huruf b harus melampirkan:
 - a. surat permohonan Nama Domain Instansi yang digunakan untuk layanan administrasi pemerintahan nasional atau layanan publik nasional;
 - b. dasar hukum yang menjadi ketentuan penyelenggaraan layanan administrasi pemerintahan nasional atau layanan publik nasional;
 - c. keterangan mengenai layanan administrasi pemerintahan nasional atau layanan publik nasional yang meliputi jenis layanan dan penerima manfaat layanan;
 - d. surat penunjukan Pejabat Nama Domain; dan
 - e. kartu aparatur sipil negara, kartu anggota TNI, kartu anggota POLRI, atau kartu identitas pegawai tetap Pejabat Nama Domain.
- (5) Pengajuan pendaftaran Nama Domain .go.id yang digunakan untuk kegiatan berskala nasional atau internasional sebagaimana dimaksud dalam Pasal 32 ayat (3) huruf c harus melampirkan:
 - a. surat permohonan Nama Domain Instansi yang digunakan untuk kegiatan berskala nasional atau internasional;
 - b. dasar hukum yang menjadi ketentuan penyelenggaraan kegiatan berskala nasional atau internasional;
 - c. keterangan mengenai kegiatan berskala nasional atau internasional;
 - d. surat penunjukan Pejabat Nama Domain; dan
 - e. kartu aparatur sipil negara, kartu anggota TNI, kartu anggota POLRI, atau kartu identitas pegawai tetap Pejabat Nama Domain.

Pasal 39

- (1) Pemerintah Daerah kabupaten/kota harus mendaftarkan Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa yang digunakan untuk alamat elektronik resmi.
- (2) Pendaftaran Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa oleh Pemerintah Daerah kabupaten/kota sebagaimana dimaksud pada ayat (1) diajukan kepada Direktur Jenderal melalui Pejabat Instansi.
- (3) Pemerintah Desa berkoordinasi dengan Pemerintah Daerah kabupaten/kota di wilayahnya dalam hal pendaftaran Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa.
- (4) Format penulisan Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa harus terdiri dari karakter yang dapat berupa:
 - a. nama atau singkatan nama; atau
 - b. akronim,dari alamat elektronik resmi Pemerintah Desa sebagaimana dimaksud dalam Pasal 32 ayat (4).
- (5) Pengajuan pendaftaran Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa oleh Pejabat Instansi sebagaimana dimaksud pada ayat (2) harus melampirkan:
 - a. surat permohonan Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa dari Pejabat Instansi atas nama bupati/walikota kepada Direktur Jenderal;
 - b. dasar hukum peraturan daerah kabupaten/kota tentang pembentukan pemerintahan desa di kabupaten/kota;
 - c. surat penunjukan Pejabat Nama Domain;
 - d. surat kuasa dari kepala desa untuk menyerahkan pendaftaran Nama Domain Pemerintah Desa pada Pejabat Nama Domain; dan
 - e. kartu aparatur sipil negara Pejabat Nama Domain pada Pemerintah Daerah kabupaten/kota.

Pasal 40

- (1) Surat penunjukan Pejabat Nama Domain sebagaimana dimaksud dalam Pasal 38 ayat (3) huruf c, ayat (4) huruf d, ayat (5) huruf d, dan Pasal 39 ayat (5) huruf c ditetapkan oleh Pejabat Instansi.
- (2) Pejabat Nama Domain yang ditetapkan oleh Pejabat Instansi sebagaimana dimaksud pada ayat (1) merupakan aparatur sipil negara yang menduduki paling rendah:
 - a. jabatan administrator pada satuan kerja atau perangkat daerah yang membidangi urusan komunikasi dan informatika; atau
 - b. jabatan fungsional ahli madya yang memiliki kompetensi bidang teknologi informasi dan

komunikasi di satuan kerja atau perangkat daerah yang membidangi urusan komunikasi dan informatika.

- (3) Surat penunjukan sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
 - a. nama pegawai; dan
 - b. nomor induk pegawai.

Pasal 41

- (1) Direktur Jenderal berwenang menyetujui atau menolak permohonan pendaftaran Nama Domain Instansi paling lama 5 (lima) hari kerja setelah permohonan pendaftaran secara elektronik diterima.
- (2) Direktur Jenderal dapat menolak permohonan pendaftaran Nama Domain dalam hal:
 - a. tidak memenuhi persyaratan sebagaimana dimaksud dalam Pasal 38 untuk Nama Domain .go.id atau Pasal 39 untuk Nama Domain .desa.id;
 - b. permohonan yang diajukan bukan berasal dari Instansi dan/atau menjadi kewenangan Instansi sesuai dengan ketentuan peraturan perundang-undangan;
 - c. Nama Domain Instansi yang diajukan telah digunakan oleh Instansi lain; dan/atau
 - d. Nama Domain Instansi yang diajukan bertentangan dengan ketentuan peraturan perundang-undangan.

Pasal 42

Nama Domain Instansi yang telah disetujui oleh Direktur dapat digunakan oleh Instansi sejak Nama Domain tersebut disetujui dan diaktifkan.

Pasal 43

Dalam hal Nama Domain Instansi telah disetujui sebagaimana dimaksud dalam Pasal 42, Pejabat Nama Domain harus memberikan informasi paling sedikit mengenai:

- a. Nama Domain yang akan didaftarkan;
- b. zona domain;
- c. nama *server*;
- d. lokasi *server hosting*;
- e. alamat protokol internet; dan
- f. *Domain Name System Security Extension (DNSSEC)*.

Paragraf 2

Perpanjangan Nama Domain Instansi

Pasal 44

- (1) Instansi harus melakukan perpanjangan Nama Domain Instansi yang masih digunakan.
- (2) Perpanjangan Nama Domain Instansi sebagaimana dimaksud pada ayat (1) untuk:
 - a. Nama Domain .go.id dilakukan oleh Pejabat Nama

- Domain Instansi; atau
- b. Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa dilakukan oleh Pejabat Nama Domain Pemerintah Daerah kabupaten/kota.
- (3) Perpanjangan sebagaimana dimaksud pada ayat (1) dilakukan paling lambat 35 (tiga puluh lima) hari kalender sejak masa berlaku Nama Domain Instansi berakhir.

Paragraf 3

Penonaktifan dan Penghapusan Nama Domain Instansi

Pasal 45

- (1) Direktur Jenderal berwenang melakukan penonaktifan Nama Domain Instansi.
- (2) Penonaktifan sebagaimana dimaksud pada ayat (1) dilakukan dalam hal:
 - a. Instansi tidak melakukan perpanjangan Nama Domain Instansi paling lambat 35 (tiga puluh lima) hari kalender terhitung sejak berakhirnya masa aktif Nama Domain Instansi tersebut;
 - b. Nama Domain Instansi dalam proses penyelesaian perselisihan;
 - c. Nama Domain Instansi berstatus dalam pengawasan karena mengalami masalah penyalahgunaan
 - d. dilakukan dengan adanya itikad tidak baik;
 - e. melanggar hak pihak lain; dan/atau
 - f. melanggar kepatutan yang berlaku dalam masyarakat atau ketentuan peraturan perundang-undangan.
- (3) Direktur Jenderal menyampaikan pemberitahuan kepada Pejabat Nama Domain melalui sarana komunikasi elektronik paling lambat 5 (lima) hari kerja sebelum melakukan penonaktifan sebagaimana dimaksud pada ayat (1) dan berkoordinasi dengan Registri Nama Domain.

Pasal 46

- (1) Direktur Jenderal memberikan rekomendasi penghapusan Nama Domain Instansi kepada Registri Nama Domain.
- (2) Pemberian rekomendasi penghapusan Nama Domain Instansi sebagaimana dimaksud pada ayat (1) dilakukan dalam hal:
 - a. proses penyelesaian perselisihan Nama Domain Instansi memutuskan penghapusan;
 - b. adanya keputusan pengadilan atau arbitrase yang bersifat final dan mengikat;
 - c. Nama Domain Instansi tidak dilakukan perpanjangan dalam kurun waktu 1 (satu) tahun sejak tanggal penonaktifan;

- d. permintaan resmi Pejabat Instansi untuk penghapusan Nama Domain .go.id;
 - e. adanya kesepakatan yang memiliki akibat hukum pembatalan penggunaan Nama Domain Instansi terdaftar oleh pihak lain; dan/atau
 - f. permintaan resmi Pejabat Instansi kabupaten/kota untuk penghapusan Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa.
- (3) Registri Nama Domain harus melaksanakan penghapusan Nama Domain Instansi sesuai rekomendasi Direktur.
 - (4) Penghapusan Nama Domain Instansi sebagaimana dimaksud pada ayat (3) dilakukan dengan cara menghapus Nama Domain Instansi dari file zona Nama Domain .id.

Pasal 47

- (1) Instansi dapat menggunakan Nama Domain Instansi yang sudah dihapus.
- (2) Dalam hal Instansi menggunakan Nama Domain Instansi yang sudah dihapus sebagaimana dimaksud pada ayat (1), Instansi harus melakukan pendaftaran Nama Domain Instansi sebagaimana dimaksud dalam Pasal 38 untuk Nama Domain .go.id atau Pasal 39 untuk Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa.

Paragraf 4

Perubahan Nama Domain Instansi

Pasal 48

- (1) Instansi dapat mengajukan perubahan Nama Domain Instansi yang digunakan.
- (2) Dalam hal terjadi perubahan Nama Domain .go.id, Instansi harus menyampaikan surat yang ditandatangani oleh Pejabat Instansi dan ditujukan kepada Direktur Jenderal.
- (3) Dalam hal terjadi perubahan Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa, Pemerintah Daerah kabupaten/kota harus menyampaikan surat yang ditandatangani oleh Pejabat Instansi dan ditujukan kepada Direktur Jenderal.
- (4) Ketentuan mengenai:
 - a. format penulisan Nama Domain;
 - b. format karakter Nama Domain; dan
 - c. pengajuan pendaftaran Nama Domain, untuk Nama Domain .go.id sebagaimana dimaksud dalam Pasal 38 dan untuk Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa sebagaimana dimaksud dalam Pasal 39 berlaku secara mutatis mutandis terhadap perubahan

Nama Domain Instansi.

Pasal 49

- (1) Instansi yang melakukan perubahan Nama Domain Instansi sebagaimana dimaksud dalam Pasal 48 dapat menggunakan Nama Domain sebelum perubahan secara bersamaan.
- (2) Penggunaan Nama Domain Instansi sebelum perubahan sebagaimana dimaksud pada ayat (1) paling lama 2 (dua) tahun sejak penetapan perubahan Nama Domain Instansi.

Pasal 50

- (1) Direktur Jenderal berwenang menyetujui atau menolak pengajuan perubahan Nama Domain Instansi paling lama 4 (empat) hari kerja sejak pengajuan secara elektronik.
- (2) Direktur Jenderal dapat menolak permohonan perubahan Nama Domain dalam hal:
 - a. tidak memenuhi persyaratan sebagaimana dimaksud dalam Pasal 38 untuk Nama Domain .go.id atau Pasal 39 untuk Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa;
 - b. permohonan yang diajukan bukan berasal dari Instansi dan/atau menjadi kewenangan Instansi sesuai dengan ketentuan peraturan perundang-undangan;
 - c. Nama Domain Instansi yang diajukan telah digunakan oleh Instansi lain; dan/atau
 - d. Nama Domain Instansi yang diajukan bertentangan dengan ketentuan peraturan perundang-undangan.
- (3) Dalam hal permohonan pengajuan perubahan Nama Domain Instansi ditolak sebagaimana dimaksud pada ayat (1), Instansi dapat mengajukan kembali permohonan pengajuan perubahan Nama Domain Instansi.

Paragraf 5

Perubahan Data Pejabat Nama Domain Instansi

Pasal 51

- (1) Dalam hal terdapat perubahan data Pejabat Nama Domain, Instansi harus mengajukan perubahan data Pejabat Nama Domain melalui Pejabat Instansi.
- (2) Perubahan data Pejabat Nama Domain sebagaimana dimaksud pada ayat (1) disampaikan kepada Direktur dengan mengirimkan surat permohonan perubahan data Pejabat Nama Domain yang ditandatangani oleh Pejabat Instansi.
- (3) Surat permohonan perubahan data Pejabat Nama Domain sebagaimana dimaksud pada ayat (2), harus disertai dengan surat penunjukan sebagaimana

dimaksud dalam Pasal 40.

Pasal 52

- (1) Direktur Jenderal dapat menyetujui permohonan pengajuan perubahan data Pejabat Nama Domain dalam hal memenuhi ketentuan Pasal 51.
- (2) Dalam hal permohonan pengajuan perubahan data Pejabat Nama Domain tidak memenuhi ketentuan Pasal 51, Direktur Jenderal berhak menolak permohonan pengajuan perubahan data Pejabat Nama Domain.
- (3) Persetujuan atau penolakan sebagaimana dimaksud pada ayat (1) dan ayat (2) diberikan paling lama 4 (empat) hari kerja sejak pengajuan permohonan perubahan data diterima secara elektronik.
- (4) Dalam hal permohonan pengajuan perubahan data Pejabat Nama Domain ditolak sebagaimana dimaksud pada ayat (2), Instansi dapat mengajukan kembali permohonan pengajuan perubahan data Pejabat Nama Domain.

Paragraf 6

Pengalihan Nama Domain Instansi

Pasal 53

- (1) Instansi dapat melakukan pengalihan Nama Domain Instansi.
- (2) Pengalihan Nama Domain Instansi sebagaimana dimaksud pada ayat (1) dilakukan dalam hal:
 - a. perubahan Instansi pengelola Nama Domain Instansi;
 - b. menggunakan Nama Domain Instansi yang sama; dan
 - c. Nama Domain Instansi yang dialihkan masih dalam masa aktif.
- (3) Pengalihan Nama Domain Instansi sebagaimana dimaksud pada ayat (1) disampaikan kepada Direktur dengan mengirimkan:
 - a. surat permohonan pengalihan Nama Domain Instansi;
 - b. surat serah terima pengalihan Nama Domain Instansi; dan
 - c. dokumen yang dipersyaratkan sebagaimana dimaksud dalam Pasal 38 untuk Nama Domain .go.id atau Pasal 39 untuk Nama Domain .desa.id.
- (4) Surat permohonan pengalihan Nama Domain Instansi dan surat serah terima pengalihan Nama Domain Instansi sebagaimana dimaksud pada ayat (3) huruf a dan huruf b ditandatangani oleh Pejabat Instansi.

Paragraf 7
Pembatalan Nama Domain Instansi

Pasal 54

- (1) Nama Domain Instansi dapat dibatalkan penggunaannya oleh Direktur Jenderal.
- (2) Pembatalan Nama Domain Instansi dilakukan pada saat Nama Domain Instansi:
 - a. didaftarkan; atau
 - b. masih digunakan.
- (3) Pembatalan Nama Domain Instansi sebagaimana dimaksud pada ayat (2) dilakukan berdasarkan permohonan dari Instansi pemohon.
- (4) Pengajuan permohonan pembatalan Nama Domain sebagaimana dimaksud pada ayat (3) disampaikan melalui surat resmi yang ditandatangani Pejabat Instansi kepada Direktur.

Paragraf 8
Pemulihan Nama Domain Instansi

Pasal 55

- (1) Instansi dapat mengajukan permohonan pemulihan Nama Domain Instansi kepada Direktur Jenderal.
- (2) Permohonan pemulihan Nama Domain sebagaimana dimaksud pada ayat (1) dilakukan melalui tahapan:
 - a. Pejabat Instansi mengajukan permohonan kepada Direktur Jenderal; dan
 - b. permohonan pemulihan Nama Domain sebagaimana dimaksud pada ayat (1) diajukan dengan melampirkan:
 1. surat permohonan tertulis;
 2. surat pernyataan telah melakukan perbaikan berdasarkan sebab penonaktifan Nama Domain sebagaimana dimaksud dalam Pasal 45 ayat (2); dan
 3. dokumen yang membuktikan telah dilakukan perbaikan sebagaimana dimaksud dalam angka 2.

Paragraf 9
Penanganan Keluhan Nama Domain Instansi

Pasal 56

- (1) Direktur Jenderal menyediakan layanan penanganan keluhan Nama Domain Instansi secara elektronik.
- (2) Layanan penanganan keluhan Nama Domain Instansi secara elektronik sebagaimana dimaksud pada ayat (1) memuat paling sedikit:
 - a. nomor kontak narahubung;
 - b. alamat surat elektronik (*email*) narahubung;
 - c. pertanyaan yang sering diajukan; dan
 - d. sistem tiket pengajuan layanan.

- (3) Instansi dan/atau publik yang menyampaikan keluhan Nama Domain Instansi melalui layanan penanganan keluhan Nama Domain Instansi secara elektronik harus mencantumkan paling sedikit:
 - a. nama pelapor;
 - b. asal Instansi/organisasi/masyarakat umum;
 - c. nomor kontak;
 - d. alamat pelapor;
 - e. nomor kartu identitas; dan
 - f. deskripsi keluhan.
- (4) Direktur Jenderal dapat berkoordinasi dengan Registri Nama Domain dalam penanganan keluhan Nama Domain Instansi.

Paragraf 10 Pemantauan dan Evaluasi

Pasal 57

- (1) Pemantauan dan evaluasi atas pengelolaan Nama Domain Instansi dilakukan oleh Direktur Jenderal.
- (2) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) dilakukan terhadap Nama Domain yang diatur dalam Peraturan Menteri ini.
- (3) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) dilakukan melalui koordinasi dengan Registri Nama Domain.
- (4) Hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (2) digunakan sebagai bahan pertimbangan pengelolaan Nama Domain Instansi.
- (5) Hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (2) dilaporkan kepada Menteri melalui Direktur Jenderal paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Bagian Keempat Penggunaan *Server* Nama Domain Instansi

Pasal 58

- (1) Instansi yang menggunakan Nama Domain Instansi harus menggunakan *server* Nama Domain yang berada di wilayah hukum Negara Kesatuan Republik Indonesia.
- (2) Instansi harus menggunakan *server* Nama Domain yang disediakan oleh Kementerian untuk Nama Domain .go.id.
- (3) Pemerintah Desa dapat menggunakan *server* Nama Domain yang disediakan oleh Kementerian untuk Nama Domain .desa.id dan/atau Nama Domain lain terkait penyebutan lain dari desa.
- (4) Instansi yang menggunakan *server* Nama Domain Instansi harus menggunakan alamat protokol internet (*IP address*) yang berada di wilayah hukum Negara Kesatuan Republik Indonesia.

Bagian Kelima
Penyelesaian Perselisihan Nama Domain Instansi

Pasal 59

- (1) Perselisihan Nama Domain Instansi merupakan perselisihan atas Nama Domain Instansi yang didaftarkan menurut Peraturan Menteri ini.
- (2) Perselisihan Nama Domain Instansi sebagaimana dimaksud pada ayat (1) dalam hal:
 - a. Nama Domain Instansi identik dan/atau memiliki kemiripan dengan Nama Domain Instansi lain; dan/atau
 - b. Nama Domain Instansi digunakan oleh Instansi lain.
- (3) Dalam hal perselisihan Nama Domain Instansi melibatkan pihak selain Instansi, penyelesaian perselisihan Nama Domain Instansi dilaksanakan berdasarkan ketentuan yang diatur oleh Registri Nama Domain.
- (4) Instansi mengajukan permohonan penyelesaian perselisihan Nama Domain Instansi kepada Direktur Jenderal melalui layanan resmi yang diselenggarakan oleh Kementerian.
- (5) Mekanisme penyelesaian perselisihan Nama Domain Instansi melalui tahapan:
 - a. Direktur Jenderal menerima permohonan penyelesaian perselisihan Nama Domain Instansi yang diajukan Instansi;
 - b. Direktur Jenderal bersama Registri Nama Domain melakukan pembahasan atas permohonan penyelesaian perselisihan Nama Domain Instansi;
 - c. penyelesaian perselisihan Nama Domain Instansi ditetapkan oleh Direktur Jenderal; dan
 - d. penetapan perselisihan Nama Domain Instansi disampaikan Direktur Jenderal kepada Instansi yang terlibat perselisihan.

BAB VI
KLASIFIKASI DATA SESUAI RISIKO PENYELENGGARA
SISTEM ELEKTRONIK LINGKUP PUBLIK

Bagian Kesatu
Umum

Pasal 60

Ruang lingkup pengaturan Klasifikasi Data Sesuai Risiko PSE Lingkup Publik meliputi:

- a. Data Terklasifikasi;
- b. pelaksana Klasifikasi Data Sesuai Risiko;
- c. pelaksanaan Klasifikasi Data Sesuai Risiko;
- d. pengelolaan, pemrosesan, dan/atau penyimpanan Data Terklasifikasi;
- e. tindak lanjut Klasifikasi Data Sesuai Risiko; dan

f. retensi Data Terklasifikasi.

Pasal 61

Dalam melakukan Klasifikasi Data Sesuai Risiko, PSE Lingkup Publik minimal harus:

- a. memastikan Data Elektronik dapat diakses oleh pihak yang berwenang sesuai dengan ketentuan peraturan perundang-undangan; dan
- b. memastikan kerahasiaan dan keamanan Data Elektronik yang dikelola, diproses, dan/atau disimpan di Pusat Data nasional dan Instansi.

Pasal 62

- (1) PSE Lingkup Publik wajib melakukan Klasifikasi Data Sesuai Risiko.
- (2) Klasifikasi Data Sesuai Risiko yang dilakukan PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) menjadi dasar untuk pengelolaan, pemrosesan, dan/atau penyimpanan Data Elektronik di Pusat Data nasional dan/atau Instansi.
- (3) Klasifikasi Data Sesuai Risiko sebagaimana dimaksud pada ayat (1) dilakukan terhadap Data Elektronik yang dikelola oleh PSE Lingkup Publik.
- (4) Klasifikasi Data Sesuai Risiko sebagaimana dimaksud pada ayat (1) dilakukan dengan tahapan:
 - a. penetapan area dampak risiko;
 - b. penetapan kriteria dampak; dan
 - c. penentuan level risiko,sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 63

- (1) PSE Lingkup Publik harus menggunakan Data Terklasifikasi yang menjadi bagian dari daftar data yang ditetapkan oleh pimpinan Instansi atau kepala daerah sesuai dengan ketentuan peraturan perundang-undangan bidang satu data Indonesia.
- (2) Dalam hal Data Terklasifikasi sebagaimana dimaksud pada ayat (1) belum ditetapkan oleh pimpinan Instansi atau kepala daerah, pembahasan Data Terklasifikasi dilaksanakan melalui mekanisme Forum Satu Data Indonesia sesuai dengan ketentuan peraturan perundang-undangan bidang satu data Indonesia.
- (3) Dalam hal pembahasan Data Terklasifikasi sebagaimana dimaksud pada ayat (2) terdapat perselisihan, penyelesaian perselisihan dilaksanakan melalui mekanisme Forum Satu Data Indonesia tingkat pusat.
- (4) Hasil pembahasan Klasifikasi Data Sesuai Risiko sebagaimana dimaksud ayat (2) dilaporkan kepada Forum Satu Data Indonesia tingkat pusat.
- (5) Hasil pembahasan Klasifikasi Data Sesuai Risiko sebagaimana dimaksud ayat (3) mencakup daftar Data yang menjadi Data Prioritas yang selanjutnya ditetapkan

menteri yang menyelenggarakan urusan pemerintahan di bidang perencanaan pembangunan nasional.

- (6) Ketentuan lebih lanjut terkait dengan penyelenggaraan Forum Satu Data Indonesia tingkat pusat dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan bidang satu data Indonesia.

Bagian Kedua Data Terklasifikasi

Pasal 64

- (1) Data Terklasifikasi terdiri atas:
 - a. Data Elektronik terbuka;
 - b. Data Elektronik terbatas; dan
 - c. Data Elektronik tertutup.
- (2) Data Elektronik terbuka sebagaimana dimaksud pada ayat (1) huruf a memiliki level risiko rendah.
- (3) Data Elektronik terbatas sebagaimana dimaksud pada ayat (1) huruf b memiliki level risiko sedang.
- (4) Data Elektronik tertutup sebagaimana dimaksud pada ayat (1) huruf c memiliki level risiko tinggi.
- (5) Data terklasifikasi sebagaimana dimaksud pada ayat (1) merupakan Arsip sesuai dengan ketentuan peraturan perundang-undangan mengenai kearsipan.

Bagian Ketiga Pelaksana Klasifikasi Data Sesuai Risiko

Paragraf 1

Pelaksana Klasifikasi Data Sesuai Risiko Instansi Pusat

Pasal 65

Pelaksanaan Klasifikasi Data Sesuai Risiko Instansi Pusat dilakukan oleh pelaksana Klasifikasi Data Sesuai Risiko Instansi Pusat yang terdiri atas:

- a. pimpinan Instansi Pusat;
- b. Pejabat Instansi;
- c. Pembina Data;
- d. Walidata tingkat pusat;
- e. Produsen Data tingkat pusat;
- f. forum satu data Instansi Pusat; dan
- g. Forum Satu Data Indonesia tingkat pusat.

Pasal 66

Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, pimpinan Instansi Pusat sebagaimana dimaksud dalam Pasal 65 huruf a mempunyai fungsi:

- a. menetapkan Data Terklasifikasi;
- b. menetapkan hasil Reklasifikasi Data; dan
- c. memberikan persetujuan Akses Data Elektronik untuk Data Elektronik tertutup.

Pasal 67

- (1) Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Pejabat Instansi sebagaimana dimaksud dalam Pasal 65 huruf b mempunyai fungsi:
 - a. mengoordinasikan pelaksanaan Klasifikasi Data Sesuai Risiko minimal mengenai:
 1. penyusunan inventaris Data Elektronik yang akan dilakukan klasifikasi;
 2. jadwal pelaksanaan klasifikasi; dan
 3. proses penetapan Data Terklasifikasi.
 - b. memberikan persetujuan atas usulan Peninjauan Kembali; dan
 - c. menyampaikan Data Terklasifikasi dan hasil Reklasifikasi Data kepada pimpinan Instansi Pusat untuk ditetapkan.
- (2) Pejabat Instansi sebagaimana dimaksud ayat (1) merupakan koordinator forum satu data Instansi Pusat sesuai dengan ketentuan peraturan perundang-undangan bidang satu data Indonesia.

Pasal 68

Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Pembina Data sebagaimana dimaksud dalam Pasal 65 huruf c memiliki fungsi memberikan rekomendasi dan pembinaan Klasifikasi Data Sesuai Risiko dalam lingkup penyelenggaraan satu data Indonesia.

Pasal 69

- (1) Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Walidata tingkat pusat sebagaimana dimaksud dalam Pasal 65 huruf d mempunyai fungsi:
 - a. mengumpulkan Data Terklasifikasi dari Produsen Data tingkat pusat;
 - b. melakukan verifikasi terhadap Data Terklasifikasi dan hasil Reklasifikasi Data;
 - c. melakukan validasi Data Terklasifikasi dan hasil Reklasifikasi Data;
 - d. mengelompokkan Data Elektronik sesuai Data Terklasifikasi;
 - e. mengelompokkan Data Terklasifikasi berdasarkan Reklasifikasi Data;
 - f. membuat dan memperbarui daftar Data Terklasifikasi;
 - g. mengelola Data Terklasifikasi yang telah ditetapkan oleh pimpinan Instansi Pusat;
 - h. menyampaikan daftar Data Terklasifikasi dan hasil Reklasifikasi Data kepada Pejabat Instansi;
 - i. menyusun telaah kebutuhan Peninjauan Kembali;
 - j. menyampaikan usulan Peninjauan Kembali atas Data Terklasifikasi;
 - k. memberikan persetujuan Akses untuk Data Elektronik terbatas; dan
 - l. membantu Produsen Data tingkat pusat dalam

melakukan Klasifikasi Data Sesuai Risiko dan Reklasifikasi Data.

- (2) Daftar Data Terklasifikasi sebagaimana dimaksud pada ayat (1) huruf f memuat minimal:
 - a. kode referensi;
 - b. kelompok Data Terklasifikasi;
 - c. nama Data Elektronik;
 - d. bulan penetapan Data Terklasifikasi; dan
 - e. tahun penetapan Data Terklasifikasi.
- (3) Walidata tingkat pusat sebagaimana dimaksud ayat (1) merupakan Walidata tingkat pusat sesuai dengan ketentuan peraturan perundang-undangan bidang satu data Indonesia.

Pasal 70

Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Produsen Data tingkat pusat sebagaimana dimaksud dalam Pasal 65 huruf e mempunyai fungsi:

- a. melakukan Klasifikasi Data Sesuai Risiko;
- b. melakukan Reklasifikasi Data; dan
- c. menyampaikan Data Terklasifikasi dan hasil Reklasifikasi Data kepada Walidata tingkat pusat untuk diverifikasi dan divalidasi.

Pasal 71

Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, forum satu data Instansi Pusat sebagaimana dimaksud dalam Pasal 65 huruf f memiliki fungsi wadah komunikasi dan koordinasi internal terkait pembahasan Klasifikasi Data Sesuai Risiko

Pasal 72

Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Forum Satu Data Indonesia tingkat pusat sebagaimana dimaksud dalam Pasal 65 huruf g memiliki fungsi sebagai wadah pelaporan hasil Data Terklasifikasi yang telah ditetapkan oleh pimpinan Instansi pusat.

Paragraf 2

Pelaksana Klasifikasi Data Sesuai Risiko Pemerintah Daerah

Pasal 73

Pelaksanaan Klasifikasi Data Sesuai Risiko Pemerintah Daerah dilakukan oleh:

- a. kepala daerah;
- b. Pejabat Instansi;
- c. Pembina Data tingkat daerah;
- d. Walidata tingkat daerah;
- e. Walidata Pendukung;
- f. Produsen Data tingkat daerah;
- g. Forum Satu Data Indonesia tingkat daerah; dan
- h. Forum Satu Data Indonesia tingkat pusat.

Pasal 74

Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, kepala daerah sebagaimana dimaksud dalam Pasal 73 huruf a mempunyai fungsi:

- a. menetapkan Data Terklasifikasi dan hasil Reklasifikasi Data; dan
- b. memberikan persetujuan Akses Data Elektronik untuk Data Elektronik tertutup.

Pasal 75

(1) Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Pejabat Instansi sebagaimana dimaksud dalam Pasal 73 huruf b mempunyai fungsi:

- a. mengoordinasikan pelaksanaan Klasifikasi Data Sesuai Risiko paling sedikit mengenai:
 1. penyusunan inventaris Data Elektronik yang akan dilakukan klasifikasi;
 2. jadwal pelaksanaan klasifikasi; dan
 3. proses penetapan Data Terklasifikasi.
 - b. menyampaikan Data Terklasifikasi dan hasil Reklasifikasi Data ke kepala daerah untuk ditetapkan; dan
 - c. memberikan persetujuan atas usulan Peninjauan Kembali.
- (2) Pejabat Instansi sebagaimana dimaksud ayat (1) merupakan koordinator Forum Satu Data Indonesia tingkat daerah sesuai dengan ketentuan peraturan perundang-undangan bidang satu data Indonesia.

Pasal 76

Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Pembina Data tingkat daerah sebagaimana dimaksud dalam Pasal 73 huruf c memiliki fungsi memberikan rekomendasi dan pembinaan Klasifikasi Data Sesuai Risiko dalam lingkup penyelenggaraan satu data indonesia tingkat daerah.

Pasal 77

(1) Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Walidata tingkat daerah sebagaimana dimaksud dalam Pasal 73 huruf d mempunyai fungsi:

- a. mengumpulkan Data Terklasifikasi dari Produsen Data tingkat daerah;
- b. membantu Produsen Data tingkat daerah dalam melakukan Klasifikasi Data Sesuai Risiko dan Reklasifikasi Data;
- c. melakukan pengecekan kesesuaian proses Klasifikasi Data Sesuai Risiko dengan pedoman klasifikasi data Pemerintah Daerah;
- d. melakukan verifikasi terhadap Data Terklasifikasi dan hasil Reklasifikasi Data;
- e. melakukan validasi Data Terklasifikasi dan hasil Reklasifikasi Data;
- f. mengelompokkan Data Terklasifikasi;

- g. membuat dan memperbarui daftar Data Terklasifikasi;
 - h. mengelola Data Terklasifikasi yang telah ditetapkan oleh kepala daerah;
 - i. mengajukan usulan Peninjauan Kembali atas Data Terklasifikasi; dan
 - j. memberikan persetujuan Akses untuk Data Elektronik terbatas.
- (2) Daftar Data Terklasifikasi sebagaimana dimaksud pada ayat (1) huruf g paling sedikit memuat:
- a. kode Referensi;
 - b. kelompok Data Terklasifikasi;
 - c. nama Data;
 - d. bulan penetapan Data Terklasifikasi; dan
 - e. tahun penetapan Data Terklasifikasi.
- (3) Walidata tingkat daerah sebagaimana dimaksud ayat (1) merupakan Walidata tingkat daerah sesuai dengan ketentuan peraturan perundang-undangan bidang satu data indonesia.

Pasal 78

Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Walidata Pendukung sebagaimana dimaksud dalam Pasal 73 huruf e memiliki fungsi membantu Walidata tingkat daerah.

Pasal 79

Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Produsen Data tingkat daerah sebagaimana dimaksud dalam Pasal 73 huruf f mempunyai fungsi:

- a. melakukan Klasifikasi Data Sesuai Risiko;
- b. melakukan Reklasifikasi Data; dan
- c. menyampaikan Data Terklasifikasi dan hasil Reklasifikasi Data kepada Walidata tingkat daerah untuk diverifikasi dan divalidasi.

Pasal 80

Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Forum Satu Data Indonesia tingkat daerah sebagaimana dimaksud dalam Pasal 73 huruf g, memiliki fungsi wadah komunikasi dan koordinasi internal daerah terkait pembahasan Klasifikasi Data Sesuai Risiko.

Pasal 81

Dalam pelaksanaan Klasifikasi Data Sesuai Risiko, Forum Satu Data Indonesia tingkat pusat sebagaimana dimaksud dalam Pasal 73 huruf h, memiliki fungsi sebagai wadah pelaporan hasil Data Terklasifikasi yang telah ditetapkan oleh kepala daerah.

Bagian Keempat
Pelaksanaan Klasifikasi Data Sesuai Risiko

Paragraf 1
Pelaksanaan Klasifikasi Data Sesuai Risiko Instansi Pusat

Pasal 82

- (1) Pelaksanaan Klasifikasi Data Sesuai Risiko Instansi Pusat harus terdokumentasi.
- (2) Pimpinan Instansi Pusat menetapkan Data Terklasifikasi.
- (3) Pelaksanaan Klasifikasi Data tingkat pusat melibatkan Forum Satu Data Instansi Pusat.

Paragraf 2
Pelaksanaan Klasifikasi Data Sesuai Risiko
Pemerintah Daerah

Pasal 83

- (1) Pelaksanaan Klasifikasi Data Sesuai Risiko Pemerintah Daerah harus terdokumentasi.
- (2) Pelaksanaan Klasifikasi Data Sesuai Risiko Pemerintah Daerah harus memperhatikan pedoman klasifikasi data Pemerintah Daerah yang diterbitkan oleh menteri yang menyelenggarakan urusan dalam negeri setelah berkoordinasi dengan Menteri dan menteri yang menyelenggarakan urusan perencanaan pembangunan.
- (3) Kepala daerah menetapkan Data Terklasifikasi dengan keputusan kepala daerah.
- (4) Pelaksanaan Klasifikasi Data Sesuai Risiko tingkat daerah melibatkan Forum Satu Data Indonesia tingkat daerah.

Paragraf 3
Peninjauan Kembali dan Reklasifikasi Data

Pasal 84

- (1) Penetapan Data Terklasifikasi sebagaimana dimaksud dalam Pasal 82 ayat (2) dan Pasal 83 ayat (3) dapat dilakukan Peninjauan Kembali dan Reklasifikasi Data.
- (2) Peninjauan Kembali sebagaimana dimaksud pada ayat (1) dilakukan secara periodik:
 - a. 1 (satu) kali dalam 3 (tiga) tahun untuk Data Elektronik terbuka;
 - b. 1 (satu) kali dalam 5 (lima) tahun untuk Data Elektronik terbatas; dan
 - c. 1 (satu) kali dalam 15 (lima belas) tahun untuk Data Elektronik tertutup.
- (3) Peninjauan Kembali sebagaimana dimaksud pada ayat (2) dapat dilakukan sewaktu-waktu sesuai kebutuhan berdasarkan:
 - a. penilaian ulang tingkat risiko;
 - b. hasil pemantauan dan evaluasi pelaksanaan

- Klasifikasi Data Sesuai Risiko;
- c. perubahan kebijakan nasional; dan/atau
 - d. perubahan proses bisnis.
- (4) Hasil Peninjauan Kembali sebagaimana dimaksud pada ayat (3) meliputi:
- a. Reklasifikasi Data; atau
 - b. Mempertahankan tingkat Klasifikasi Data Sesuai Risiko.
- (5) Reklasifikasi Data sebagaimana dimaksud pada ayat (4) huruf a dapat:
- a. menaikkan tingkat Data Terklasifikasi; atau
 - b. menurunkan tingkat Data Terklasifikasi.

Pasal 85

Pimpinan Instansi Pusat menetapkan hasil perubahan Reklasifikasi Data.

Pasal 86

Kepala daerah menetapkan hasil perubahan Reklasifikasi Data.

Bagian Kelima

Pengelolaan, Pemrosesan, dan/atau Penyimpanan Data Terklasifikasi

Pasal 87

- (1) PSE Lingkup Publik wajib melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Data Terklasifikasi di wilayah Negara Kesatuan Republik Indonesia dengan memastikan kontrol dan tindakan keamanan yang sesuai.
- (2) Pengelolaan, pemrosesan, dan/atau penyimpanan Data Terklasifikasi sebagaimana dimaksud pada ayat (1) dilakukan di:
 - a. Pusat Data nasional; dan/atau
 - b. Instansi.
- (3) Pengelolaan, pemrosesan, dan/atau penyimpanan Data Terklasifikasi sebagaimana dimaksud pada ayat (2) harus memperhatikan:
 - a. Data Elektronik terbuka dan terbatas ditempatkan di Pusat Data nasional; dan
 - b. Data Elektronik tertutup ditempatkan di Pusat Data nasional dan/atau Instansi.
- (4) Pengelolaan, pemrosesan, dan/atau penyimpanan Data Elektronik terbuka dan terbatas sebagaimana dimaksud pada ayat (3) huruf a dilakukan di Pusat Data nasional yang terdiri atas:
 - a. layanan fasilitas Pusat Data pemerintah;
 - b. layanan Komputasi Awan pemerintah; dan
 - c. layanan pihak ketiga yang terlibat dalam penyelenggaraan Pusat Data nasional sesuai ketentuan peraturan perundang-undangan.
- (5) Pengelolaan, pemrosesan, dan/atau penyimpanan Data Elektronik tertutup sebagaimana dimaksud pada ayat (3)

huruf b dilakukan di:

- a. layanan fasilitas Pusat Data pemerintah; atau
- b. wadah penyimpanan yang ditempatkan di pusat komputasi Instansi.

Pasal 88

- (1) Dalam hal teknologi penyimpanan tidak tersedia di dalam negeri, PSE Lingkup Publik dapat melakukan pengelolaan, pemrosesan, dan/atau penyimpanan Sistem Elektronik dan Data Elektronik di luar wilayah Negara Kesatuan Republik Indonesia.
- (2) Kriteria teknologi penyimpanan tidak tersedia di dalam negeri sebagaimana dimaksud pada ayat (1) ditentukan oleh komite yang terdiri atas Kementerian, lembaga yang membidangi urusan pengkajian dan penerapan teknologi, lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan sandi, dan Kementerian atau Lembaga terkait.
- (3) Komite sebagaimana dimaksud pada ayat (2) ditetapkan oleh Menteri.

Pasal 89

- (1) Dalam hal Data Elektronik tertutup disimpan di Instansi sebagaimana dimaksud dalam Pasal 87 ayat (3) huruf b, Instansi harus menyediakan dan menggunakan wadah penyimpanan media terenkripsi.
- (2) Wadah penyimpanan media terenkripsi sebagaimana dimaksud pada ayat (1) ditempatkan di pusat komputasi milik Instansi.
- (3) Pengelolaan, pemrosesan, dan/atau penyimpanan Data Elektronik tertutup di Pusat Data Instansi harus memenuhi ketentuan persyaratan Akses Data Terklasifikasi sesuai dengan ketentuan dalam Peraturan Menteri ini.

Pasal 90

Data Elektronik terbatas dan tertutup disimpan (*at-rest*) dalam keadaan terenkripsi.

Bagian Keenam

Tindak Lanjut Klasifikasi Data Sesuai Risiko

Paragraf 1

Pengiriman Data Elektronik di Dalam Jaringan

Pasal 91

- (1) Pengiriman Data Elektronik di dalam jaringan untuk Data Elektronik terbuka sebagaimana dimaksud dalam Pasal 64 ayat (1) huruf a harus memperhatikan keaslian dan keutuhan Data Elektronik.
- (2) Pengiriman Data Elektronik di dalam jaringan untuk Data Elektronik terbatas sebagaimana dimaksud dalam Pasal 64 ayat (1) huruf b paling sedikit dilakukan:

- a. dengan menjamin keaslian dan keutuhan Data Elektronik;
 - b. melalui jaringan intra pemerintah; dan
 - c. dengan dikirimkan (*in-transit*) dalam keadaan terenkripsi.
- (3) Data Elektronik tertutup sebagaimana dimaksud dalam Pasal 64 ayat (1) huruf c tidak dapat dibagipakaikan melalui jaringan.
 - (4) Dalam hal Data Elektronik sebagaimana dimaksud pada ayat (1) sampai dengan ayat (3) merupakan Data Elektronik strategis, Instansi atau Institusi harus membuat dokumen elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu sesuai dengan ketentuan peraturan perundang-undangan.

Paragraf 2

Pengiriman Data Elektronik di Luar Jaringan

Pasal 92

- (1) Dalam hal pengiriman Data Elektronik di dalam jaringan terdapat kendala dan/atau ukuran file terlalu besar untuk diakses, maka dapat dilakukan pengiriman Data di luar jaringan.
- (2) Pengiriman Data Elektronik di luar jaringan untuk Data Elektronik terbuka harus memperhatikan keaslian dan keutuhan Data Elektronik.
- (3) Pengiriman Data Elektronik di luar jaringan untuk Data Elektronik terbatas memerlukan:
 - a. enkripsi pada Data Elektronik di dalam media dengan menggunakan algoritma kriptografi yang tidak dipublikasikan yang disediakan oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan sandi; dan
 - b. wadah penyimpanan media yang disegel dan diberi label “Terbatas” yang disediakan oleh Instansi yang membutuhkan Data Elektronik.
- (4) Pengiriman Data Elektronik tertutup tidak dapat dikirimkan di luar jaringan dan/atau media apapun.

Paragraf 3

Persyaratan Akses Data Terklasifikasi

Pasal 93

- (1) Akses terhadap Data Terklasifikasi dapat diberikan sesuai dengan persyaratan Akses.
- (2) Akses terhadap Data Elektronik terbuka harus memenuhi persyaratan:
 - a. tetap memperhatikan keaslian dan keutuhan Data Elektronik; dan
 - b. dapat diunduh dan disimpan di banyak media.
- (3) Akses terhadap Data Elektronik terbatas harus memenuhi persyaratan:

- a. mendapat persetujuan Walidata; dan
 - b. dapat diunduh dan disimpan dalam media terenkripsi.
- (4) Walidata sebagaimana dimaksud pada ayat (3) huruf a harus melakukan pengawasan terhadap Akses Data Terklasifikasi.
- (5) Persyaratan Persetujuan sebagaimana dimaksud pada ayat (3) huruf a ditentukan oleh Instansi pemilik Data Elektronik.
- (6) Akses terhadap Data Elektronik tertutup harus memenuhi persyaratan:
- a. mendapat izin tertulis dari pimpinan Instansi pemilik Data Elektronik;
 - b. Akses diberikan hanya untuk pejabat negara dan/atau ASN/TNI/POLRI dengan jabatan paling rendah pimpinan tinggi pratama yang ditunjuk oleh pimpinan Instansi pemilik Data Elektronik;
 - c. tersedia ruangan khusus untuk mengakses Data Elektronik;
 - d. Akses Data Elektronik hanya dapat dilakukan pada waktu tertentu dan diberi pembatasan waktu Akses sesuai dengan kebijakan yang ditetapkan bersama oleh pengelola Pusat Data nasional dan/atau Instansi sebagai pemilik Data Elektronik;
 - e. Akses Data Elektronik dapat dilakukan melalui perangkat yang sudah terdaftar di Instansi;
 - f. Data Elektronik hanya dapat dibaca (*read only*) oleh pihak yang telah ditunjuk sebagaimana dimaksud dalam huruf b;
 - g. harus dilakukan pengawasan terhadap semua Akses oleh pimpinan Instansi pemilik Data Elektronik; dan
 - h. harus melalui proses pengajuan Akses Data Elektronik.
- (7) Persyaratan izin tertulis sebagaimana dimaksud pada ayat (6) huruf a ditentukan oleh Instansi pemilik Data Elektronik.
- (8) Spesifikasi ruangan khusus sebagaimana dimaksud pada ayat (6) huruf c meliputi:
- a. penerapan perimeter keamanan;
 - b. penjagaan ruangan khusus dengan mekanisme kontrol keamanan yang tepat;
 - c. perancangan dan penerapan keamanan fisik untuk kantor, ruangan dan fasilitas ruangan khusus;
 - d. perancangan dan penerapan perlindungan fisik terhadap bencana alam, serangan berbahaya, dan kejadian tidak terduga;
 - e. perancangan dan penerapan prosedur untuk bekerja di ruangan khusus; dan
 - f. penentuan titik Akses di mana pihak yang tidak berwenang dapat memasuki ruangan khusus harus dikendalikan dan diisolasi untuk menghindari

Akses yang tidak sah.

- (9) Proses pengajuan Akses Data Elektronik sebagaimana dimaksud pada ayat (6) huruf h dilakukan dengan mengajukan surat permohonan kepada pengelola Pusat Data nasional dan/atau Instansi sebagai pemilik Data Elektronik dengan mencantumkan:
 - a. profil pejabat negara dan/atau ASN/TNI/POLRI dengan jabatan paling rendah jabatan pimpinan tinggi pratama yang ditunjuk oleh pimpinan Instansi pemilik Data Elektronik;
 - b. waktu Akses Data Elektronik;
 - c. data perangkat yang akan digunakan untuk melakukan Akses Data Elektronik; dan
 - d. izin tertulis dari pimpinan Instansi Pusat atau kepala daerah.

Bagian Ketujuh Retensi Data Terklasifikasi

Pasal 94

- (1) Retensi Data Terklasifikasi merupakan penyimpanan atas Data Terklasifikasi.
- (2) Jangka waktu retensi Data Terklasifikasi ditetapkan oleh Instansi pemilik Data sesuai dengan ketentuan peraturan perundang-undangan.
- (3) Instansi pemilik Data Elektronik menetapkan retensi Data Terklasifikasi, sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 95

- (1) Instansi pemilik Data harus melakukan pemusnahan Data Terklasifikasi secara aman sesuai dengan ketentuan peraturan perundang-undangan.
- (2) Pemusnahan Data Terklasifikasi sebagaimana dimaksud pada ayat (1) termasuk memastikan pemusnahan Data Terklasifikasi yang dikuasai oleh Penyedia layanan Komputasi Awan pihak ketiga.
- (3) Pemusnahan Data Terklasifikasi sebagaimana dimaksud pada ayat (2) harus memenuhi persyaratan:
 - a. telah habis retensi;
 - b. tidak memiliki nilai guna;
 - c. sesuai dengan ketentuan peraturan perundang-undangan; dan
 - d. tidak berkaitan dengan penyelesaian proses suatu perkara.

Bagian Kedelapan Layanan Komputasi Awan

Pasal 96

- (1) PSE Lingkup Publik harus memanfaatkan layanan Komputasi Awan yang diselenggarakan di Pusat Data nasional.

- (2) Layanan Komputasi Awan yang diselenggarakan di Pusat Data nasional sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. layanan Komputasi Awan pemerintah; dan
 - b. layanan Komputasi Awan pihak ketiga, yang memenuhi persyaratan tertentu sesuai dengan ketentuan peraturan perundang-undangan.
- (3) Layanan Komputasi Awan pemerintah sebagaimana dimaksud pada ayat (2) huruf a merupakan layanan pemanfaatan berbagipakai data aplikasi dan infrastruktur oleh Instansi melalui jaringan intra pemerintah atau jaringan internet yang diamankan yang disediakan oleh Kementerian.
- (4) Layanan Komputasi Awan pihak ketiga sebagaimana dimaksud pada ayat (2) huruf b diselenggarakan oleh Penyedia layanan Komputasi Awan pihak ketiga yang terdaftar di Kementerian.
- (5) Pusat Data nasional sebagaimana dimaksud pada ayat (2) huruf a dan huruf c saling terhubung.
- (6) Penyedia layanan Komputasi Awan pihak ketiga yang terdaftar di Kementerian sebagaimana dimaksud pada ayat (4) harus dapat diaudit sesuai dengan ketentuan peraturan perundang-undangan.
- (7) Dalam hal PSE Lingkup Publik menggunakan Penyedia layanan Komputasi Awan pihak ketiga, PSE Lingkup Publik wajib melakukan Klasifikasi Data Sesuai Risiko atas Data Elektronik yang dikelolanya sebagaimana dimaksud dalam Pasal 64.
- (8) Pedoman penyelenggaraan Pusat Data nasional sebagaimana dimaksud pada ayat (1) ditetapkan oleh Menteri.

Pasal 97

- (1) Menteri menerbitkan daftar Penyedia layanan Komputasi Awan pihak ketiga yang terdaftar di Kementerian sebagaimana dimaksud dalam Pasal 96 ayat (4).
- (2) Penyedia layanan Komputasi Awan pihak ketiga yang terdaftar di Kementerian sebagaimana dimaksud pada ayat (1) harus memenuhi persyaratan.
- (3) Ketentuan mengenai persyaratan sebagaimana dimaksud pada ayat (2) ditetapkan oleh Menteri.

Pasal 98

- (1) Format:
 - a. surat tugas pejabat pendaftar PSE Lingkup Publik yang berasal dari Instansi sebagaimana dimaksud dalam Pasal 6 ayat (2);
 - b. surat tugas pejabat pendaftar PSE Lingkup Publik yang berasal dari Institusi sebagaimana dimaksud dalam Pasal 7 ayat (2);
 - c. surat keterangan Sistem Elektronik yang sudah

tidak digunakan sebagaimana dimaksud dalam Pasal 15;

- d. laman labuh (*landing page*) sebagaimana dimaksud dalam Pasal 28;
- e. karakter yang dapat berupa nama atau singkatan nama atau akronim dari nama resmi Instansi sebagaimana dimaksud dalam Pasal 38 ayat (2) huruf a;
- f. karakter Nama Domain *.desa.id* dan/atau Nama Domain lain terkait penyebutan lain dari desa sebagaimana dimaksud dalam Pasal 39 ayat (4);
- g. surat serah terima pengalihan Nama Domain Instansi sebagaimana dimaksud dalam Pasal 53 ayat (3) huruf b; dan
- h. surat permohonan pengajuan penyelesaian perselisihan Nama Domain Instansi sebagaimana dimaksud dalam Pasal 59 ayat (4),

tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(2) Contoh:

- a. Nama Domain Instansi yang digunakan untuk alamat elektronik resmi Instansi sebagaimana dimaksud dalam Pasal 32 ayat (3) huruf a;
- b. Nama Domain Instansi yang digunakan untuk layanan administrasi pemerintahan nasional atau layanan publik nasional sebagaimana dimaksud dalam Pasal 32 ayat (3) huruf b;
- c. Nama Domain Instansi yang digunakan untuk kegiatan berskala nasional dan/atau internasional sebagaimana dimaksud dalam Pasal 32 ayat (3) huruf c; dan
- d. Nama Domain Instansi yang digunakan untuk alamat elektronik resmi Pemerintah Desa sebagaimana dimaksud dalam Pasal 32 ayat (4),

tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(3) Mekanisme terkait:

- a. Tahapan Klasifikasi Data Sesuai Risiko sebagaimana dimaksud dalam Pasal 62 ayat (4);
- b. Penetapan Klasifikasi Data Sesuai Risiko sebagaimana dimaksud dalam Pasal 63 ayat (1);
- c. Pelaksanaan Klasifikasi Data Sesuai Risiko Instansi Pusat sebagaimana dimaksud dalam Pasal 82;
- d. Pelaksanaan Klasifikasi Data Sesuai Risiko Pemerintah Daerah sebagaimana dimaksud dalam Pasal 83;
- e. Pelaksanaan Peninjauan Kembali dan Reklasifikasi Data Instansi tingkat pusat sebagaimana dimaksud dalam Pasal 85; dan
- f. Pelaksanaan Peninjauan Kembali dan Reklasifikasi Data Instansi tingkat daerah sebagaimana dimaksud dalam Pasal 86,

tercantum dalam Lampiran III yang merupakan bagian

tidak terpisahkan dari Peraturan Menteri ini.

BAB VII PEMBINAAN DAN PENGAWASAN

Bagian Kesatu Pembinaan

Pasal 99

- (1) Menteri melakukan pembinaan terhadap penyelenggaraan Sistem Elektronik lingkup publik.
- (2) Pembinaan terhadap PSE Lingkup Publik sebagaimana dimaksud pada ayat (1) dilakukan terhadap:
 - a. pejabat pendaftar PSE Lingkup Publik;
 - b. pejabat nama domain; dan
 - c. walidata.
- (3) Pembinaan sebagaimana dimaksud pada ayat (1) dilakukan dalam bentuk kegiatan fasilitasi, konsultasi, pendidikan dan pelatihan, dan/atau pengembangan.

Bagian Kedua Pengawasan

Pasal 100

- (1) Menteri melakukan pengawasan terhadap penyelenggaraan Sistem Elektronik lingkup publik.
- (2) Pengawasan sebagaimana dimaksud pada ayat (1) mencakup pemantauan, pengendalian, pemeriksaan, penelusuran, dan pengamanan.

BAB VIII KETENTUAN PERALIHAN

Pasal 101

- (1) PSE Lingkup Publik yang telah menyelenggarakan Sistem Elektronik sebelum Peraturan Menteri ini berlaku, wajib melakukan pendaftaran paling lambat 1 (satu) tahun sejak Peraturan Menteri ini mulai berlaku.
- (2) PSE Lingkup Publik yang telah melakukan pendaftaran sebelum Peraturan Menteri ini berlaku, wajib melakukan pendaftaran sesuai dengan ketentuan dalam Peraturan Menteri ini paling lambat 1 (satu) tahun sejak Peraturan Menteri ini mulai berlaku.
- (3) PSE Lingkup Publik wajib menyesuaikan penyelenggaraan Sistem Elektroniknya sesuai dengan ketentuan dalam peraturan Menteri ini paling lambat 1 (satu) tahun sejak Peraturan Menteri ini mulai berlaku.

Pasal 102

PSE Lingkup Publik yang menggunakan Penyedia layanan Komputasi Awan pihak ketiga sebelum Peraturan Menteri ini berlaku harus menggunakan Penyedia layanan Komputasi Awan pihak ketiga yang terdaftar di Kementerian paling

lambat:

- a. 1 (satu) tahun sejak Menteri menerbitkan daftar Penyedia layanan Komputasi Awan pihak ketiga sebagaimana dimaksud dalam Pasal 97 ayat (1); atau
- b. setelah masa kontrak PSE Lingkup Publik dengan Penyedia layanan Komputasi Awan pihak ketiga sebelumnya berakhir.

BAB IX KETENTUAN PENUTUP

Pasal 103

Pada saat Peraturan Menteri ini mulai berlaku:

- a. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2015 tentang Registrar Nama Domain Instansi Penyelenggara Negara (Berita Negara Republik Indonesia Nomor 209); dan
- b. Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2015 tentang Tata Cara Pendaftaran Sistem Elektronik Instansi Penyelenggara Negara (Berita Negara Republik Indonesia Nomor 320),
dicabut dan dinyatakan tidak berlaku.

Pasal 104

Peraturan Menteri ini mulai berlaku sejak tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Menteri ini dengan penempatannya dalam Berita Negara Republik Indonesia.



Ditetapkan di Jakarta
pada tanggal 18 Maret 2025

MENTERI KOMUNIKASI DAN DIGITAL
REPUBLIK INDONESIA,

☐

MEUTYA VIADA HAFID

Diundangkan di Jakarta
pada tanggal ☐

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM REPUBLIK INDONESIA,

☐

DHAHANA PUTRA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2025 NOMOR ☐

LAMPIRAN I
PERATURAN MENTERI
KOMUNIKASI DAN DIGITAL
REPUBLIK INDONESIA
NOMOR 5 TAHUN 2025
TENTANG
PENYELENGGARA SISTEM ELEKTRONIK
LINGKUP PUBLIK

FORMAT SURAT TUGAS
PEJABAT PENDAFTAR PSE LINGKUP PUBLIK YANG BERASAL DARI INSTANSI

[KOP SURAT]

SURAT TUGAS

Nomor :

- Menimbang : 1. bahwa dalam rangka melaksanakan Pendaftaran atas Sistem Elektronik yang dikelola PSE Lingkup Publik sebagaimana diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dipandang perlu untuk menunjuk pejabat pendaftar Penyelenggara Sistem Elektronik Lingkup Publik;
- Mengingat : 1. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
2. ... dst;
- Kepada : Nama : [nama Pejabat Pendaftar PSE Lingkup Publik]
NIP : [NIP Pejabat Pendaftar PSE Lingkup Publik]
Jabatan : [nama Jabatan]
Unit Kerja : [nama Unit Kerja/Satker/Perangkat Daerah Pejabat Pendaftar PSE Lingkup Publik].
- Untuk : 1. melaksanakan proses Pendaftaran atas Sistem Elektronik yang dikelola Penyelenggara Sistem Elektronik Lingkup Publik;
2. memastikan kebenaran seluruh data Pendaftaran atas Sistem Elektronik yang dikelola Penyelenggara Sistem Elektronik Lingkup Publik;
3. melakukan pemutakhiran data Pendaftaran atas Sistem Elektronik yang dikelola Penyelenggara Sistem Elektronik Lingkup Publik;
4. menjaga kerahasiaan akses yang terdiri atas

username dan *password* serta data Pendaftaran atas Sistem Elektronik yang dikelola Penyelenggara Sistem Elektronik Lingkup Publik;

5. memberikan informasi pelaksanaan sistem pengamanan dalam penyelenggaraan Sistem Elektronik; dan
6. melaporkan hasil kegiatan Pendaftaran atas Sistem Elektronik yang dikelola Penyelenggara Sistem Elektronik Lingkup Publik kepada Pejabat Instansi.

Dikeluarkan di : [Nama Kota Instansi]

Tanggal : [Tanggal Surat Tugas]

[Jabatan Pejabat Instansi]

[Nama Pejabat Instansi]

NIP: [NIP Pejabat Instansi]

xxxxxx

FORMAT SURAT TUGAS PEJABAT PENDAFTAR PSE LINGKUP PUBLIK YANG
BERASAL DARI INSTITUSI

[KOP SURAT]

SURAT TUGAS

Nomor :

- Menimbang : bahwa dalam rangka melaksanakan Pendaftaran atas Sistem Elektronik yang dikelola PSE Lingkup Publik sebagaimana diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dipandang perlu untuk menunjuk pejabat pendaftar Penyelenggara Sistem Elektronik Lingkup Publik;
- Mengingat : 1. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
2..... dst;
- Kepada : Nama : [nama pejabat pendaftar PSE Lingkup Publik]
Nomor Pegawai : [Nomor Pegawai pejabat pendaftar PSE Lingkup Publik]
Jabatan : [nama Jabatan]
Unit Kerja : [nama Unit Kerja/Satker/pejabat pendaftar PSE Lingkup Publik].
- Untuk : 1. melaksanakan proses Pendaftaran atas Sistem Elektronik yang dikelola Penyelenggara Sistem Elektronik Lingkup Publik;
2. memastikan kebenaran dan keakuratan seluruh data pendaftaran Penyelenggara Sistem Elektronik Lingkup Publik;
3. melakukan pemutakhiran data Pendaftaran atas Sistem Elektronik yang dikelola Penyelenggara Sistem Elektronik Lingkup Publik;
4. menjaga kerahasiaan akses yang terdiri atas *username* dan *password* serta data Pendaftaran atas Sistem Elektronik yang dikelola Penyelenggara Sistem Elektronik Lingkup Publik;
5. memberikan informasi pelaksanaan sistem pengamanan dalam penyelenggaraan Sistem Elektronik; dan

6. melaporkan hasil kegiatan Pendaftaran atas Sistem Elektronik yang dikelola Penyelenggara Sistem Elektronik Lingkup Publik kepada [pimpinan di institusi].

Dikeluarkan di : [Nama Kota Institusi]

Tanggal : [Tanggal Surat Tugas]

[Jabatan Pimpinan Institusi]

[Nama Pimpinan Institusi]
[Nomor Pegawai Pimpinan Institusi]

FORMAT SURAT KETERANGAN SISTEM ELEKTRONIK TIDAK DIGUNAKAN
[KOP SURAT]

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama :

NIP :

Jabatan :

Pangkat/Golongan :

Dengan ini menyatakan bahwa Sistem Elektronik di bawah ini:

1...

2...

3...

Dst..

sudah tidak digunakan dalam penyelenggaraan Sistem Elektronik Lingkup Publik di lingkungan [Nama Instansi].

Surat keterangan ini dibuat dengan sebenarnya untuk digunakan sebagai kelengkapan dokumen dalam proses penghapusan Tanda Daftar PSE Lingkup Publik.

Demikian disampaikan, atas perhatiannya diucapkan terima kasih.

[Jabatan Pejabat Instansi]

[Nama Pejabat Instansi]

NIP: [NIP Pejabat Instansi]

FORMAT LAMAN LABUH (LANDING PAGE)



FORMAT KARAKTER NAMA DOMAIN INSTANSI DAN PEMERINTAH DESA

1. Nama domain go.id dan desa.id terdiri dari minimal 3 (tiga) karakter dan maksimal 63 (enam puluh tiga) karakter (huruf, angka, tanda minus/penghubung).
2. Nama Domain terdiri atas huruf (A-Z, a-z), angka (0-9) dan karakter *hyphen* (“-“). Karakter *hyphen* tidak boleh digunakan sebagai awal atau akhir, serta sebagai karakter ketiga dan keempat secara berurutan, dari suatu Nama Domain.
3. Nama Domain dapat diawali dengan huruf dan diikuti dengan angka atau diawali dengan angka dan diikuti dengan huruf. Nama Domain tidak dapat hanya menggunakan angka untuk seluruh Nama Domain.
4. Kementerian memiliki kewenangan untuk menolak usulan Nama Domain yang dinilai tidak mengakomodasi asas kepatutan umum dalam pengelolaan Nama Domain.

FORMAT SURAT SERAH TERIMA PENGALIHAN NAMA DOMAIN INSTANSI

[Kop Surat Instansi Pihak Pertama]

BERITA ACARA SERAH TERIMA
PENGALIHAN NAMA DOMAIN INSTANSI

Nomor:.....[nomor BAST sesuai nomenklatur penomoran instansi]

Pada hari ini tanggal bulan tahun[tanggal, bulan, tahun ditulis dalam bentuk huruf], kami yang bertanda tangan di bawah ini:

Nama :[nama pejabat Pejabat Instansi]
Instansi :[nama instansi]
Jabatan :[nama jabatan sekretaris jenderal/ sekretaris utama/ sekretaris daerah/ pejabat yang memimpin unit sekretariat di Instansi]
Alamat :[alamat instansi]
Selanjutnya disebut PIHAK PERTAMA;

Nama :[nama pejabat Pejabat Instansi]
Instansi :[nama instansi]
Jabatan :[nama jabatan sekretaris jenderal/ sekretaris utama/ sekretaris daerah/ pejabat yang memimpin unit sekretariat di Instansi]
Alamat :[alamat instansi]
Selanjutnya disebut PIHAK KEDUA.

PIHAK PERTAMA dan PIHAK KEDUA secara bersama-sama disebut PARA PIHAK.

PARA PIHAK sepakat untuk melakukan serah terima Nama Domain Instansi dengan ketentuan sebagai berikut:

Pasal 1

PIHAK PERTAMA menyerahkan pengelolaan atas Nama Domain Instansi [... .go.id/ ...desa.id] kepada PIHAK KEDUA dan PIHAK KEDUA menerima pengalihan pengelolaan Nama Domain Instansi dimaksud sesuai dengan ketentuan yang berlaku.

Pasal 2

Sejak Berita Acara ini ditandatangani maka tanggung jawab pengelolaan atas nama domain sebagaimana dimaksud dalam Pasal 1 beralih dari PIHAK PERTAMA ke PIHAK KEDUA.

Pasal 3

Berita Acara serah terima ini dibuat dengan sebenarnya dalam rangkap secukupnya bermeterai dan mempunyai kekuatan hukum yang sama bagi PARA PIHAK untuk digunakan sebagaimana mestinya.

.....,

PIHAK PERTAMA
Meterai dan Ttd

PIHAK KEDUA
Ttd

.....
NIP.....

.....
NIP...

Catatan : Asli dibuat dua rangkap, rangkap kedua Meterai ditempatkan pada PIHAK KEDUA.

FORMAT SURAT PERMOHONAN PENGAJUAN PENYELESAIAN PERSELISIHAN
NAMA DOMAIN INSTANSI
[Kop Surat Instansi]

(TEMPAT DAN TANGGAL SURAT)

NOMOR :
SIFAT :
LAMPIRAN :
HAL :

Kepada Yth.
Direktur Jenderal (...)
Kementerian Komunikasi dan Digital

Kami selaku Pemohon mengajukan permohonan penyelesaian perselisihan Nama Domain instansi, dengan keterangan sebagai berikut:

nama Instansi/pemohon :
Nama Domain yang diperselisihkan :
nama Instansi/termohon :
deskripsi yang diperselisihkan :

Demikian disampaikan permohonan penyelesaian perselisihan Nama Domain instansi, atas perhatiannya diucapkan terima kasih.

(Pejabat Instansi)

(Nama)

(NIP)

MENTERI KOMUNIKASI DAN DIGITAL
REPUBLIK INDONESIA,

ttd

MEUTYA VIADA HAFID

LAMPIRAN II
PERATURAN MENTERI
KOMUNIKASI DAN DIGITAL
REPUBLIK INDONESIA
NOMOR 5 TAHUN 2025
TENTANG
PENYELENGGARA SISTEM ELEKTRONIK
LINGKUP PUBLIK

CONTOH NAMA DOMAIN INSTANSI

INSTANSI	FORMAT PENAMAAN NAMA DOMAIN
Lembaga Tinggi Negara dan Sekretariat Lembaga Tinggi Negara	<p>Format:</p> <ol style="list-style-type: none">1. Karakter nama [Lembaga Tinggi Negara].go.id2. Karakter nama [Sekretariat Jenderal]. [Lembaga Tinggi Negara].go.id <p>Contoh:</p> <ol style="list-style-type: none">a. DPR RI: dpr.go.idb. Sekretariat Jenderal DPR RI: setjen.dpr.go.id (sebagai contoh subdomain untuk membedakan penggunaan <i>email</i> antara anggota DPR dan jajaran staf di lingkungan kesekjenan DPR RI)
Legislatif Daerah dan Sekretariat Lembaga Legislatif Daerah	<p>Format:</p> <ol style="list-style-type: none">1. Karakter Nama [Lembaga Legislatif Daerah]-[lokasi keberadaan instansi yang dimaksud].go.id.2. Menjadi subdomain instansi Pemerintah Daerah Karakter nama [Sekretariat]. [Lembaga Legislatif Daerah]-[lokasi keberadaan instansi yang dimaksud].go.id <p>Contoh:</p> <ol style="list-style-type: none">a. DPRD Provinsi Kalteng: dprd-kaltengprov.go.idb. Sekretariat DPRD Provinsi Kalteng : sekretariat.dprd-kaltengprov.go.idc. (sebagai contoh subdomain untuk membedakan penggunaan <i>email</i> antara anggota DPRD dan jajaran staf di lingkungan kesekjenan DPRD).d. Dewan Perwakilan Rakyat Papua: dpr-papua.go.ide. Sekretariat DPR Papua : sekretariat.dpr-papua.go.idf. Dewan Perwakilan Rakyat Daerah Kabupaten Ponorogo : dprd-ponorogo.go.idg. Sekretariat DPRD Kabupaten Ponorogo : sekretariat.dprd-ponorogo.go.id

INSTANSI	FORMAT PENAMAAN NAMA DOMAIN
Kementerian	<p>Format: Karakter nama [Kementerian].go.id</p> <p>Contoh:</p> <ul style="list-style-type: none">a. Kementerian Perindustrian: kemenperin.go.idb. Kementerian Komunikasi dan Digital: komdigi.go.id
Lembaga Setingkat Kementerian, Instansi vertikalnya di daerah, dan instansi kewilayahan di daerah	<p>Format:</p> <ul style="list-style-type: none">1. Karakter nama [Lembaga setingkat Kementerian].go.id2. Karakter nama [(Singkatan)Lembaga Setingkat Kementerian – Lokasi Keberadaan Lembaga yang dimaksud].go.id <p>Contoh:</p> <ul style="list-style-type: none">a. Kejaksaan Agung RI: kejaksaan.go.idb. Kejaksaan Tinggi Prov DIY: kejati-diy.go.idc. Kejaksaan Negeri Kota Bekasi: kejar-bekasikota.go.idd. Pengadilan Tinggi Tata Usaha Negara Medan: pttun-medan.go.ide. Pengadilan Tinggi Agama Banjarmasin : pta-banjarmasin.go.idf. Pengadilan Agama Kota Depok: pa-depok.go.id
Instansi Pemerintah Non-Kementerian dan instansi lainnya yang dibentuk peraturan perundang-undangan	<p>Format: Karakter nama [Instansi pemerintah non kementerian].go.id</p> <p>Contoh:</p> <ul style="list-style-type: none">a. Badan Pusat Statistik: bps.go.idb. Badan Pembinaan Ideologi Pancasila: bpip.go.idc. Bank Indonesia: bi.go.id

INSTANSI	FORMAT PENAMAAN NAMA DOMAIN
<p>Komisi, Badan, lembaga, atau instansi yang dibentuk berdasarkan peraturan perundang undangan dan atau dibiayai oleh Negara, dan Sekretariatnya;</p>	<p>Format:</p> <ol style="list-style-type: none"> 1. Domain: Karakter nama [Karakter nama Komisi, Badan, Lembaga, atau Instansi].go.id; 2. Subdomainnya : Karakter nama [Tingkatan Pemerintahan atau lokasi Komisi, Badan, Lembaga atau Instansi yang dibentuk berdasarkan peraturan perundang-undangan].[Karakter nama Komisi, Badan, Lembaga, atau Instansi].go.id; <p>Contoh:</p> <ol style="list-style-type: none"> a. Komisi Penyiaran Indonesia: kpi.go.id b. Komisi Pemberantasan Korupsi: kpk.go.id c. Nama Domain: Komisi Pemilihan Umum: kpu.go.id Subdomain: KPU Provinsi Jatim: jatim.kpu.go.id KPU Kota Malang: kota-malang.kpu.go.id KPU Kabupaten Malang: kab-malang.kpu.go.id
<p>Pemerintah Daerah</p>	<p>Format:</p> <ol style="list-style-type: none"> 1. Domain: Karakter nama [pemerintah daerah, atau singkatannya, diikuti wilayah keberadaan pemerintah daerah Instansi Penyelenggara Negara].go.id 2. Subdomain: Karakter nama [perangkat daerah, unit pelaksana teknis, atau singkatannya di wilayah pemerintah daerah].go.id <p>Contoh:</p> <ol style="list-style-type: none"> a. Domain: Pemerintah Provinsi Sumatera Utara: sumutprov.go.id Subdomain: Dinas Komunikasi dan Informatika Provinsi Sumatera Utara: diskominfo.sumutprov.go.id b. Domain: Pemerintah Kota Surabaya: surabaya.go.id Subdomain: Dinas Perhubungan Kota Surabaya: dishub.surabaya.go.id Rumah Sakit Umum Daerah Kota Surabaya: rs-soewandhi.surabaya.go.id c. Domain: Pemerintah Kabupaten Minahasa Tenggara: mitrakab.go.id

INSTANSI	FORMAT PENAMAAN NAMA DOMAIN
	<p>Subdomain: Dinas Pendidikan Kabupaten Minahasa Tenggara: disdik.mitrakab.go.id</p> <p>Catatan: Selama tidak diidentifikasi atau tidak berpotensi diidentifikasi duplikasi nama, maka diizinkan tidak menggunakan istilah prov, kab atau kota.</p>

CONTOH NAMA DOMAIN PEMERINTAH DESA

INSTANSI	FORMAT PENAMAAN NAMA DOMAIN
Pemerintah Desa	<p>Format:</p> <ol style="list-style-type: none">1. Karakter nama [nama desa, atau singkatannya atau sebutan lain].desa.id2. Karakter nama [nama desa, atau singkatannya]-[nama kabupaten/kota/kecamatan lokasi desa berada].desa.id <p>Contoh:</p> <ol style="list-style-type: none">a. Desa Sukamaju Kabupaten Bogor: sukamaju-jonggol.desa.idb. Desa Sukamaju Kabupaten Bandung: sukamaju-majalaya.desa.id <p>Catatan: Bupati atau Walikota dapat mengusulkan penyeragaman nama domain desa.id di wilayahnya sesuai Peraturan Bupati atau Peraturan Walikota, dan selama Nama Domain yang dimaksud belum digunakan oleh desa yang lain.</p>

CONTOH NAMA DOMAIN LAYANAN ADMINISTRASI PEMERINTAHAN NASIONAL ATAU LAYANAN PUBLIK NASIONAL

INSTANSI	FORMAT PENAMAAN DOMAIN
Layanan Administrasi Pemerintahan Nasional	Format: Karakter nama [layanan administrasi pemerintahan].go.id, Contoh: Layanan Administrasi Kearsipan: arsip.go.id atau srikandi.arsip.go.id
Layanan Publik Nasional	Format: Karakter nama [layanan publik].go.id, Contoh: <ul style="list-style-type: none">• layanan pengaduan publik: lapor.go.id• layanan perpajakan: pajak.go.id• layanan <i>National Single Window</i>: insw.go.id atau insw.id

CONTOH NAMA DOMAIN KEGIATAN BERSKALA NASIONAL DAN/ATAU
INTERNASIONAL

INSTANSI	FORMAT PENAMAAN NAMA DOMAIN
Kegiatan Berskala Nasional dan/atau Internasional	<p>Format: Karakter nama [Kegiatan Kenegaraan].go.id, atau</p> <p>Contoh: a. kegiatan untuk Pekan Olahraga Nasional: pon.go.id b. kegiatan Musabaqah Tilawatil Quran: musabaqah.go.id</p> <p>Catatan: Dalam hal kegiatan berskala nasional dan/atau Internasional dimaksud merupakan kegiatan internasional, Nama Domain dapat menggunakan bahasa asing</p>

MENTERI KOMUNIKASI DAN DIGITAL
REPUBLIK INDONESIA,

ttd

MEUTYA VIADA HAFID

LAMPIRAN II
PERATURAN MENTERI
KOMUNIKASI DAN DIGITAL
REPUBLIK INDONESIA
NOMOR 5 TAHUN 2025
TENTANG
PENYELENGGARA SISTEM ELEKTRONIK
LINGKUP PUBLIK

TAHAPAN KLASIFIKASI DATA

A. MODEL KLASIFIKASI DATA SESUAI KONDISI DI INDONESIA

Model terminologi untuk Klasifikasi Data Sesuai Risiko dirancang berdasarkan hasil telaah dari 8 (delapan) sektor strategis di Indonesia dan praktik Klasifikasi Data Sesuai Risiko yang telah dilakukan oleh negara lain. Klasifikasi Data Sesuai Risiko pada PSE Lingkup Publik dibagi berdasarkan tingkat risiko dan ditampilkan pada Tabel 1.

Tabel 1. Kelompok Klasifikasi Data Sesuai Risiko

Kelompok Klasifikasi Data Sesuai Risiko	Definisi
Data Elektronik terbuka	Data Elektronik terbuka merupakan Data Elektronik yang memiliki level risiko rendah.
Data Elektronik terbatas	Data Elektronik terbatas merupakan Data Elektronik yang memiliki level risiko sedang.
Data Elektronik tertutup	Data Elektronik tertutup merupakan Data Elektronik yang memiliki level risiko tinggi.

B. KLASIFIKASI DATA DITINJAU DARI TINGKAT RISIKO

Klasifikasi Data Sesuai Risiko dilakukan terhadap Data Elektronik yang dikelola oleh PSE Lingkup Publik. Klasifikasi Data Sesuai Risiko dilakukan mulai dari analisis sampai dengan mitigasi risiko berdasarkan ketentuan peraturan perundang-undangan. Tahapan dalam melakukan penilaian risiko untuk menentukan Klasifikasi Data Sesuai Risiko pada PSE Lingkup Publik meliputi:

1. Penetapan Area Dampak Risiko Penyalahgunaan Data Elektronik
Penetapan area dampak risiko penyalahgunaan Data Elektronik didasarkan pada penetapan area dampak risiko. Penetapan area dampak risiko penyalahgunaan Data Elektronik bertujuan untuk mengetahui area mana saja yang terkena efek dari penyalahgunaan Data Elektronik yang ada di Instansi Pusat dan Pemerintah Daerah . Penetapan area dampak risiko penyalahgunaan Data Elektronik diawali dengan melakukan identifikasi dampak risiko penyalahgunaan Data Elektronik. Area dampak risiko penyalahgunaan Data Elektronik dapat disesuaikan dengan konteks internal dan eksternal di masing- masing Instansi Pusat dan Pemerintah Daerah. Area dampak risiko penyalahgunaan Data Elektronik yang menjadi fokus penerapan Manajemen Risiko meliputi:
 - a. Kerahasiaan, dampak risiko penyalahgunaan Data Elektronik berupa pengungkapan informasi yang tidak sah;
 - b. Integritas, dampak risiko penyalahgunaan Data Elektronik berupa modifikasi atau perusakan informasi yang tidak sah; dan
 - c. Ketersediaan, dampak risiko penyalahgunaan Data Elektronik berupa gangguan terhadap Akses untuk membuka atau menggunakan informasi.

2. Penetapan Kriteria Risiko Penyalahgunaan Data Elektronik
Penetapan kriteria risiko penyalahgunaan Data Elektronik bertujuan untuk mengukur dan menetapkan seberapa besar kemungkinan kejadian dan dampak risiko penyalahgunaan Data Elektronik yang dapat terjadi. Kriteria risiko penyalahgunaan Data Elektronik ini ditinjau secara berkala dan perlu melakukan penyesuaian dengan perubahan yang terjadi. Penetapan kriteria risiko penyalahgunaan Data Elektronik menggunakan Kriteria dampak Penyalahgunaan Data Elektronik. Penetapan kriteria dampak risiko penyalahgunaan Data Elektronik dilakukan dengan kombinasi antara Area Dampak Risiko Penyalahgunaan Data Elektronik dan level dampak. Instansi tingkat pusat dan Pemerintah Daerah menggunakan 3 (tiga) level, yang disesuaikan dengan kompleksitas risiko penyalahgunaan Data Elektronik. Untuk 3 (tiga) level dampak, dapat diuraikan sebagai berikut:
 - 1) Rendah;
 - 2) Sedang; dan
 - 3) Tinggi.Kriteria dampak risiko dapat dijabarkan untuk setiap area dampak. Berikut adalah penjabaran dari masing-masing area dampak pada Tabel 2.

Tabel 2. Kriteria Dampak Risiko Penyalahgunaan Data Elektronik

Area Dampak	Level Dampak		
	1	3	5
	Rendah	Sedang	Tinggi
Kerahasiaan	Pengungkapan informasi yang tidak sah berdampak rendah pada aktivitas dan aset individu, organisasi, atau nasional	Pengungkapan informasi yang tidak sah berdampak sedang pada aktivitas dan aset individu, organisasi, atau nasional	Pengungkapan informasi yang tidak sah berdampak tinggi pada aktivitas dan aset individu, organisasi, atau nasional
Integritas	Perubahan atau perusakan informasi berdampak rendah pada aktivitas dan aset individu, organisasi, atau nasional.	Perubahan atau perusakan informasi berdampak sedang pada aktivitas dan aset individu, organisasi, atau nasional.	Perubahan atau perusakan informasi berdampak tinggi pada aktivitas dan aset individu, organisasi, atau nasional.
Ketersediaan	Rendah, gangguan terhadap Akses untuk membuka atau menggunakan informasi berdampak rendah pada aktivitas organisasi, aset organisasi, atau individu.	Sedang, gangguan terhadap Akses untuk membuka atau menggunakan informasi berdampak sedang pada aktivitas organisasi, aset organisasi, atau individu.	Tinggi, gangguan terhadap Akses untuk membuka atau menggunakan informasi berdampak tinggi dan membahayakan aktivitas organisasi, aset organisasi, atau individu.

Area Dampak	Level Dampak		
	1	3	5
	Rendah	Sedang	Tinggi
Level Risiko	Rendah	Sedang	Tinggi
Rentang Level Risiko	3-7	8-11	12-15

Untuk menjaga konsistensi dari penilaian level dampak dari Klasifikasi Data Sesuai Risiko yang dilakukan oleh Instansi Pusat dan Pemerintah Daerah , maka pelaksana klasifikasi data dapat mengikuti dampak potensial pada Tabel 3.

Tabel 3. Dampak Potensial

Dampak Potensial	Rendah	Sedang	Tinggi
Nasional	<ul style="list-style-type: none"> • Urusan pemerintahan sehari-hari, pemberian layanan, dan keuangan publik; • hubungan internasional rutin dan kegiatan diplomatik; • Keamanan publik, peradilan pidana dan kegiatan penegakan hukum; 	<ul style="list-style-type: none"> • Keselamatan, keamanan atau kemakmuran Indonesia atau negara sahabat dengan mempengaruhi kepentingan finansial, ekonomi dan keuangan; • Keamanan dan ketahanan aset Infrastruktur Nasional yang penting; 	<ul style="list-style-type: none"> • Mengancam secara langsung stabilitas internal Indonesia atau negara sahabat; • Kerusakan jangka panjang bagi perekonomian Indonesia; • Runtuh, mati, atau gangguan besar terhadap aset

Dampak Potensial	Rendah	Sedang	Tinggi
	<ul style="list-style-type: none"> • Berefek pada aspek pertahanan, keamanan dan ketahanan; • Kepentingan finansial, termasuk informasi yang diberikan secara rahasia dan kekayaan intelektual 	<ul style="list-style-type: none"> • Efektivitas operasional pertahanan dan keamanan, termasuk kemampuan untuk menginvestigasi atau menuntut kejahatan terorganisir yang serius • Hubungan dengan pemerintah negara-negara sahabat atau merusak hubungan internasional yang mengakibatkan protes atau sanksi formal. 	<p>Infrastruktur Nasional Penting yang signifikan;</p> <ul style="list-style-type: none"> • Kerusakan yang sangat parah terhadap keefektifan pertahanan dan keamanan, termasuk kerusakan besar dalam jangka panjang terhadap kemampuan untuk menyelidiki atau menuntut kejahatan terorganisir yang serius; • Meningkatkan ketegangan internasional; • Kerusakan yang sangat parah pada hubungan dengan negara-negara sahabat.
Organisasi	Kerusakan terbatas pada operasi dan layanan bisnis rutin organisasi, termasuk: Kepentingan finansial, termasuk informasi yang	Kerusakan sedang pada operasi dan layanan rutin organisasi, termasuk penurunan yang parah atau kehilangan kemampuan	Kerusakan fatal terhadap operasi dan layanan rutin organisasi sehingga memberikan efek kepada masyarakat dan pihak luar

Dampak Potensial	Rendah	Sedang	Tinggi
	diberikan secara rahasia dan kekayaan intelektual.	organisasi.	organisasi.
Individu	Informasi pribadi yang harus dilindungi berdasarkan undang-undang perlindungan data atau undang-undang lainnya.	<ul style="list-style-type: none">• Mengancam kehidupan, kebebasan, atau keselamatan seseorang secara langsung• Diskriminasi, perlakuan buruk, penghinaan, atau pelemahan martabat atau keselamatan seseorang yang mengarah pada potensi bahaya yang signifikan atau cedera yang berpotensi mengancam nyawa.	<ul style="list-style-type: none">• Menyebabkan langsung hilangnya nyawa secara luas• Diskriminasi, perlakuan buruk, penghinaan atau perendahan martabat atau keselamatan orang yang secara wajar dapat diharapkan untuk secara langsung menyebabkan kematian sejumlah besar orang.

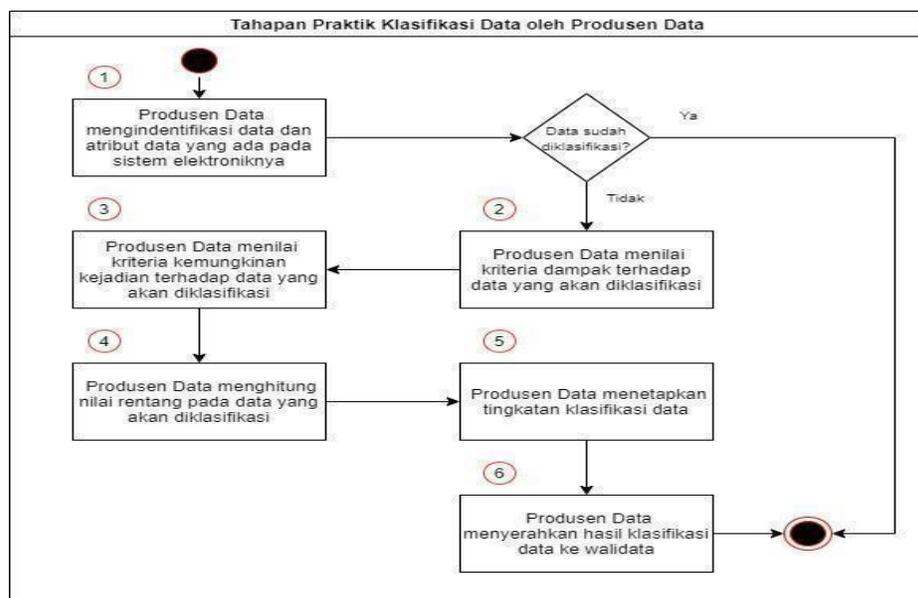
3. Penentuan level risiko pada ⁻⁷⁴⁻klasifikasi data
 Besaran risiko yang didapatkan ini selanjutnya dikelompokkan ke dalam level rentang besaran risiko sesuai kelompok klasifikasi data. Terdapat 3 (tiga) kelompok Data Terklasifikasi yaitu:
- 1) Data Elektronik terbuka;
 - 2) Data Elektronik terbatas; dan
 - 3) Data Elektronik tertutup.
- Pada Tabel 4 disampaikan nilai rentang klasifikasi data untuk 3 (tiga) kelompok. Hal ini ditujukan bagi Instansi tingkat pusat dan Pemerintah Daerah yang telah melakukan praktik Klasifikasi Data Sesuai Risiko dan menggunakan 3 (tiga) kelompok Data Terklasifikasi.

Tabel 4. Nilai Rentang Klasifikasi Data Sesuai Risiko dengan 3 (tiga) kelompok

No.	Kelompok Klasifikasi Data	Level Risiko	Nilai Rentang	Keterangan Warna
1	Terbuka	Rendah	3-7	Hijau
2	Terbatas	Sedang	8-11	Kuning
3	Tertutup	Tinggi	12-15	Merah

C. STUDI KASUS PENILAIAN RISIKO UNTUK KLASIFIKASI DATA PADA PSE LINGKUP PUBLIK

Pada bagian ini akan dijelaskan studi kasus Klasifikasi Data Sesuai Risiko pada Data Elektronik di PSE Lingkup Publik, serta tahapan yang dilakukan oleh PSE Lingkup Publik dalam melakukan Klasifikasi Data Sesuai Risiko berdasarkan penilaian risiko, yaitu pada Gambar 1.



Gambar 1. Tahapan Praktik Klasifikasi Data Sesuai Risiko oleh Produsen Data

Tahapan praktik klasifikasi data oleh Produsen Data: -75-

1. Menentukan Data Elektronik yang akan diklasifikasi

Pada tahapan ini, PSE Lingkup Publik menentukan Data Elektronik dari layanannya yang akan diklasifikasi. Data Elektronik, dengan mengidentifikasi data yang ada, termasuk:

- a. jenis data (data terstruktur, atau data tidak terstruktur);
- b. status data (data diam, atau data berjalan);
- c. nilai data (tingkat kerahasiaan dan sensitifitas terhadap pelanggaran);
- d. lokasi data (lokal atau *cloud*).

Pada studi kasus ini, akan menggunakan Data Elektronik yang berkaitan langsung dengan layanan yang dikelola oleh PSE Lingkup Publik. Berikut contoh Data Elektronik yang akan diklasifikasikan, namun untuk memudahkan justifikasi, Data Elektronik ini juga dilengkapi dengan atribut Data Elektronik.:

- a. data peminjaman ruangan
- b. data KTP
- c. data Beban Kerja Pegawai
- d. data Alat Utama Sistem Senjata (alutsista)
- e. data daftar fasilitas kesehatan
- f. data Penerima Manfaat Bantuan Sosial
- g. data undangan rapat

2. Menilai kriteria dampak terhadap Data Elektronik

PSE Lingkup Publik dapat menentukan kriteria dampak dari Data Elektronik yang akan diklasifikasi berdasarkan 3 (tiga) kriteria dampak, yaitu Kerahasiaan, Integritas, dan Ketersediaan. Pada saat menilai kriteria dampak, PSE Lingkup Publik menggunakan panduan yang telah tersedia pada Tabel 2. Kriteria Dampak Risiko Penyalahgunaan Data Elektronik. Pada Tabel 5. Penilaian Kriteria Dampak Terhadap Data Elektronik di PSE Lingkup Publik disajikan penilaian kriteria dampak terhadap Data Elektronik.

Tabel 5. Penilaian Kriteria Dampak Terhadap Data Elektronik Layanan dari IPPD

No	Data	Atribut Data (Sebagai Justifikasi)	K/L/D Pemilik Data	Area Dampak	Level Dampak	Nilai Dampak
1	Peminjaman ruangan	1. Nama peminjam 2. Tanggal pemakaian 3. Lama pemakaian 4. Tujuan pemakaian	Semua K/L/D	Kerahasiaan	Rendah	1
				Integritas	Rendah	1
				Ketersediaan	Sedang	3
2	KTP	1. Nama 2. NIK 3. Alamat 4. Tempat dan tanggal lahir 5. Agama 6. Pekerjaan	Kementerian Dalam Negeri	Kerahasiaan	Sedang	3
				Integritas	Tinggi	5
				Ketersediaan	Sedang	3

No	Data	Atribut Data (Sebagai Justifikasi)	K/L/D Pemilik Data	Area Dampak	Level Dampak	Nilai Dampak
3	Beban Kerja Pegawai	Atribut Data: 1. Fungsi unit organisasi 2. Rincian tugas 3. Jangka waktu pekerjaan 4. Jenis pekerjaan 5. Nama pegawai	BKN	Kerahasiaan	Rendah	1
				Integritas	Sedang	3
				Ketersediaan	Sedang	3
4	Alutsista	1. Nama sistem senjata 2. Pengelola 3. Jumlah 4. Lokasi penyimpanan 5. Kondisi	Kementerian Pertahanan	Kerahasiaan	Tinggi	5
				Integritas	Tinggi	5
				Ketersediaan	Tinggi	5

No	Data	Atribut Data (Sebagai Justifikasi)	K/L/D Pemilik Data	Area Dampak	Level Dampak	Nilai Dampak
5	Daftar Fasilitas Kesehatan	1. Nama faskes 2. Tipe faskes 3. Lokasi 4. Alamat 5. Kontak	Kementerian Kesehatan	Kerahasiaan	Rendah	1
				Integritas	Sedang	3
				Ketersediaan	Sedang	3
6	Penerima Manfaat Bantuan Sosial	1. Nama penerima 2. NIK 3. Tempat dan tanggal lahir 4. Alamat 5. Kontak 6. Besaran manfaat	Kementerian Sosial	Kerahasiaan	Sedang	3
				Integritas	Sedang	3
				Ketersediaan	Sedang	3

No	Data	Atribut Data (Sebagai Justifikasi)	K/L/D Pemilik Data	Area Dampak	Level Dampak	Nilai Dampak
7	Undangan Rapat	1. Hari dan tanggal 2. Waktu 3. Lokasi 4. Agenda 5. Daftar undangan	Semua K/L/D	Kerahasiaan	Rendah	1
				Integritas	Sedang	3
				Ketersediaan	Sedang	3

Dari Tabel 5 di atas, dapat dilihat salah satu Data Elektronik, yaitu Data Beban Kerja Pegawai yang diukur dampaknya jika terjadi penyalahgunaan Data Elektronik berdasarkan:

- a. Dampak Kerahasiaan:
Jika terjadi penyalahgunaan Data Elektronik Beban Kerja Pegawai, maka akan berdampak rendah pada tingkat pengungkapan informasi yang tidak sah karena data tersebut tidak termasuk data yang dirahasiakan. Oleh karena itu dampak kerahasiaan adalah tidak signifikan.
 - b. Dampak Integritas:
Jika terjadi penyalahgunaan Data Elektronik Beban Kerja Pegawai, maka akan berdampak sedang pada tingkat perubahan dan kerusakan informasi. Hal ini dikarenakan rincian tugas dan jangka waktu pekerjaan merupakan acuan dari kondisi SDM di PSE Lingkup Publik. Oleh karena itu dampak integritas adalah signifikan.
 - c. Dampak Ketersediaan:
Jika terjadi penyalahgunaan Data Elektronik Beban Kerja Pegawai, maka akan berdampak sedang pada tingkat gangguan terhadap Akses untuk membuka atau menggunakan informasi. Hal ini dikarenakan rincian tugas dan jangka waktu pekerjaan merupakan informasi yang harus dapat diakses ketika dibutuhkan. Oleh karena itu dampak ketersediaan adalah signifikan.
3. Menghitung nilai rentang pada Data Elektronik yang diklasifikasi Setelah PSE Lingkup Publik menentukan kriteria dampak, maka PSE Lingkup Publik dapat menghitung nilai rentang dan nilai total yang bersumber dari Tabel 6. Nilai Rentang dan Nilai Total dari Data Elektronik di PSE Lingkup Publik, disajikan nilai rentang dan nilai total Data Elektronik dari PSE Lingkup Publik.

Tabel 6. Nilai Rentang dan Nilai Total dari Data Elektronik di PSE Lingkup Publik

No	Data	Atribut Data (Sebagai Justifikasi)	K/L/D Pemilik Data	Area Dampak	Level Dampak	Nilai Dampak	Nilai Total
1	Peminjaman ruangan	1. Nama peminjam 2. Tanggal pemakaian 3. Lama pemakaian 4. Tujuan pemakaian	Semua K/L/D	Kerahasiaan	Rendah	1	5
				Integritas	Rendah	1	
				Ketersediaan	Sedang	3	

No	Data	Atribut Data (Sebagai Justifikasi)	K/L/D Pemilik Data	Area Dampak	Level Dampak	Nilai Dampak	Nilai Total
2	KTP	<ol style="list-style-type: none"> 1. Nama 2. NIK 3. Alamat 4. Tempat dan tanggal lahir 5. Agama 6. Pekerjaan 	Kementerian Dalam Negeri	Kerahasiaan	Sedang	3	11
				Integritas	Tinggi	5	
				Ketersediaan	Sedang	3	
3	Beban Kerja Pegawai	Atribut Data: <ol style="list-style-type: none"> 1. Fungsi unit organisasi 2. Rincian tugas 3. Jangka waktu pekerjaan 4. Jenis pekerjaan 5. Nama pegawai 	BKN	Kerahasiaan	Rendah	1	7
				Integritas	Sedang	3	
				Ketersediaan	Sedang	3	
4	Alutsista	<ol style="list-style-type: none"> 1. Nama sistem senjata 2. Pengelola 3. Jumlah 4. Lokasi penyimpanan 6. Kondisi 	Kementerian Pertahanan	Kerahasiaan	Tinggi	5	15
				Integritas	Tinggi	5	
				Ketersediaan	Tinggi	5	
5	Daftar Fasilitas Kesehatan	<ol style="list-style-type: none"> 1. Nama faskes 2. Tipe faskes 3. Lokasi 4. Alamat 5. Kontak 	Kementerian Kesehatan	Kerahasiaan	Rendah	1	7
				Integritas	Sedang	3	
				Ketersediaan	Sedang	3	

No	Data	Atribut Data (Sebagai Justifikasi)	K/L/D Pemilik Data	Area Dampak	Level Dampak	Nilai Dampak	Nilai Total
6	Penerima Manfaat Bantuan Sosial	1. Nama penerima 2. NIK 3. Tempat dan tanggal lahir 4. Alamat 5. Kontak 6. Besaran manfaat	Kementerian Sosial	Kerahasiaan	Sedang	3	9
				Integritas	Sedang	3	
				Ketersediaan	Sedang	3	
7	Undangan Rapat	1. Hari dan tanggal 2. Waktu 3. Lokasi 4. Agenda 5. Daftar undangan	Semua K/L/D	Kerahasiaan	Rendah	1	7
				Integritas	Sedang	3	
				Ketersediaan	Sedang	3	

4. Menetapkan kelompok klasifikasi data

Setelah PSE Lingkup Publik mendapatkan nilai total, maka dilanjutkan dengan memetakan nilai total dengan nilai rentang dari kelompok klasifikasi data sesuai yang tersedia pada Tabel 4. Nilai Rentang Klasifikasi Data Sesuai Risiko dengan 3 (tiga) kelompok. Pada Tabel 7. disajikan kelompok Data Terklasifikasi berdasarkan nilai total yang didapatkan.

Tabel 7. Kelompok Data Terklasifikasi di PSE Lingkup Publik

No	Data	Nilai Total	Data Terklasifikasi
1	Peminjaman ruangan	5	Terbuka
2	KTP	11	Terbatas
3	Beban Kerja Pegawai	7	Terbuka
4	Alutsista	15	Tertutup
5	Daftar Fasilitas Kesehatan	7	Terbuka

No	Data	Nilai Total	Data Terklasifikasi
6	Penerima Manfaat Bantuan Sosial	9	Terbatas
7	Undangan Rapat	7	Terbuka

Berdasarkan Tabel 7, maka kelompok Data Terklasifikasi di PSE Lingkup Publik sudah ditetapkan berdasarkan nilai total, yaitu:

- a. Data Peminjaman Ruang memiliki nilai total 5 yang merupakan kelompok Data Elektronik terbuka;
- b. Data KTP memiliki nilai total 11 yang merupakan kelompok Data Elektronik terbatas;
- c. Data Beban Kerja Pegawai memiliki nilai total 7 yang merupakan yang merupakan kelompok Data Elektronik terbuka;
- d. Data Alutsista memiliki nilai total 15 yang merupakan yang merupakan kelompok Data Elektronik tertutup;
- e. Data Daftar Fasilitas Kesehatan memiliki nilai total 7 yang merupakan kelompok Data Elektronik terbuka;
- f. Data Penerima Manfaat Bantuan Sosial memiliki nilai total 9 yang merupakan kelompok Data Elektronik terbatas; dan
- g. Data Undangan Rapat memiliki nilai total 7 yang merupakan kelompok Data Elektronik terbuka.

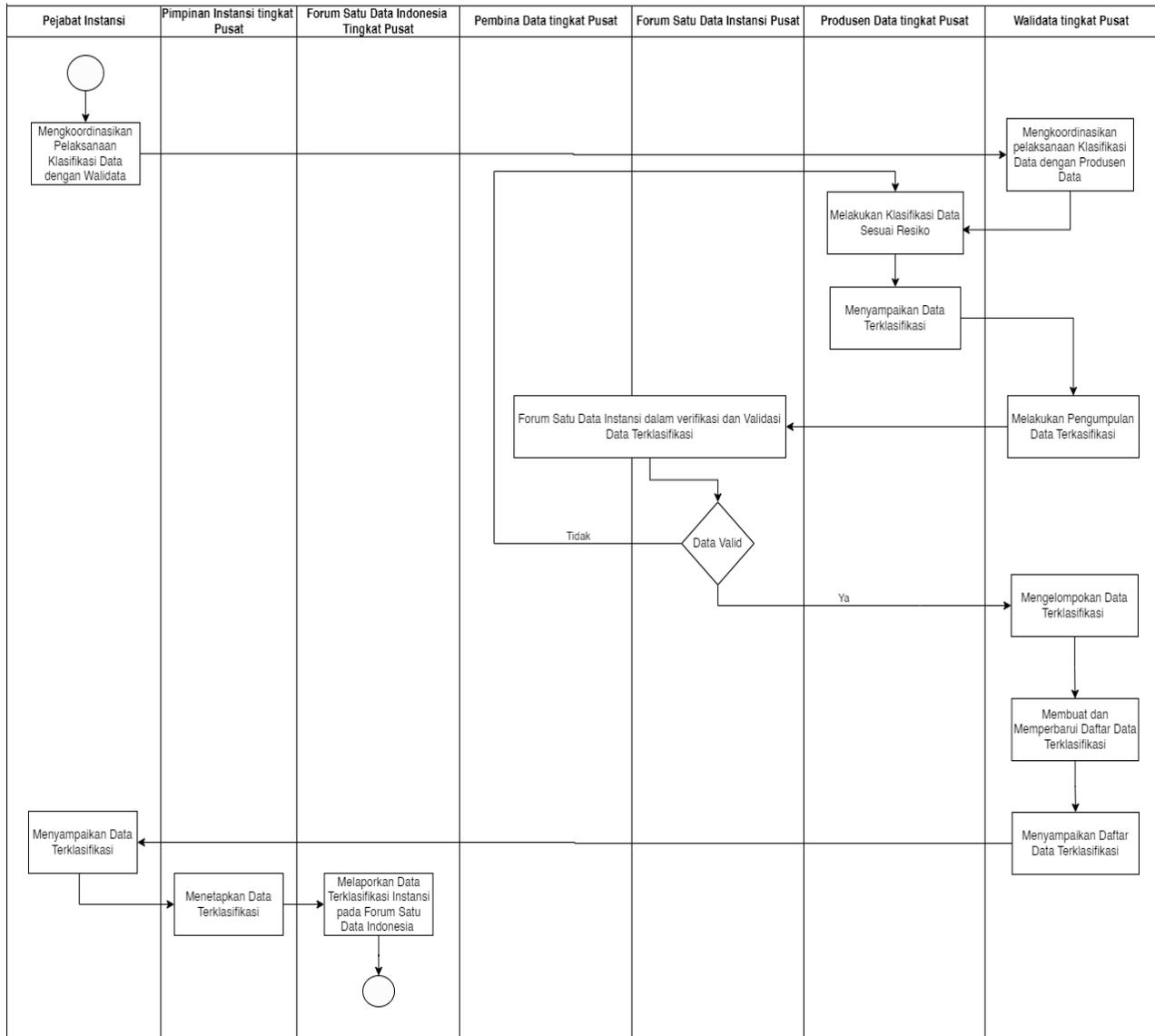
5. Menyerahkan hasil Klasifikasi Data Sesuai Risiko

Setelah PSE Lingkup Publik menetapkan Kelompok Data Terklasifikasi, maka Produsen Data akan menyerahkan hasil klasifikasi data yang telah dilakukan kepada Walidata. Walidata akan memeriksa kesesuaian hasil klasifikasi data yang telah dilakukan oleh Produsen Data.

PELAKSANAAN KLASIFIKASI DATA INSTANSI PUSAT

Mekanisme pelaksanaan Klasifikasi Data Sesuai Risiko PSE Lingkup Publik pada Instansi Pusat pada Gambar 2. sebagai berikut:

1. Pejabat Instansi mengoordinasikan pelaksanaan Klasifikasi Data Sesuai Risiko dengan Walidata tingkat pusat.
2. Walidata tingkat pusat berkoordinasi dengan Produsen Data tingkat pusat untuk melakukan Klasifikasi Data Sesuai Risiko.
3. Produsen Data tingkat pusat melakukan Klasifikasi Data Sesuai Risiko, sesuai dengan Tahapan Klasifikasi Data Sesuai Risiko, sebagai berikut:
 - a. Penetapan Area Dampak Risiko Penyalahgunaan Data Elektronik;
 - b. Penetapan Kriteria Risiko Penyalahgunaan Data Elektronik; dan
 - c. Penentuan level risiko pada klasifikasi data.
4. Produsen Data tingkat pusat menyampaikan Data Terklasifikasi kepada Walidata tingkat pusat.
5. Walidata tingkat pusat mengumpulkan Data Terklasifikasi dari Produsen Data tingkat pusat.
6. Walidata tingkat pusat bersama dengan Pembina Data tingkat pusat melakukan verifikasi dan validasi Data Terklasifikasi sesuai dengan mekanisme penilaian risiko yang disepakati dalam forum satu data Instansi Pusat. Apabila Data tidak valid maka Walidata tingkat pusat mengembalikan Data Terklasifikasi kepada Produsen Data tingkat pusat untuk dilakukan klasifikasi ulang.
7. Apabila berdasarkan verifikasi dan validasi Data Terklasifikasi valid, Walidata tingkat pusat mengelompokkan Data Elektronik sesuai kelompok Data Terklasifikasi.
8. Walidata tingkat pusat membuat dan memperbarui daftar Data Terklasifikasi.
9. Walidata tingkat pusat menyampaikan daftar Data Terklasifikasi kepada Pejabat Instansi.
10. Pejabat Instansi menyampaikan Data Terklasifikasi kepada pimpinan Instansi Pusat sebagai bahan pertimbangan penetapan Data Terklasifikasi.
11. Pimpinan Instansi Pusat menetapkan Data Terklasifikasi.
12. Hasil Data Terklasifikasi yang telah ditetapkan oleh Pimpinan Instansi tingkat pusat dilaporkan kepada Forum Satu Data Indonesia tingkat pusat.

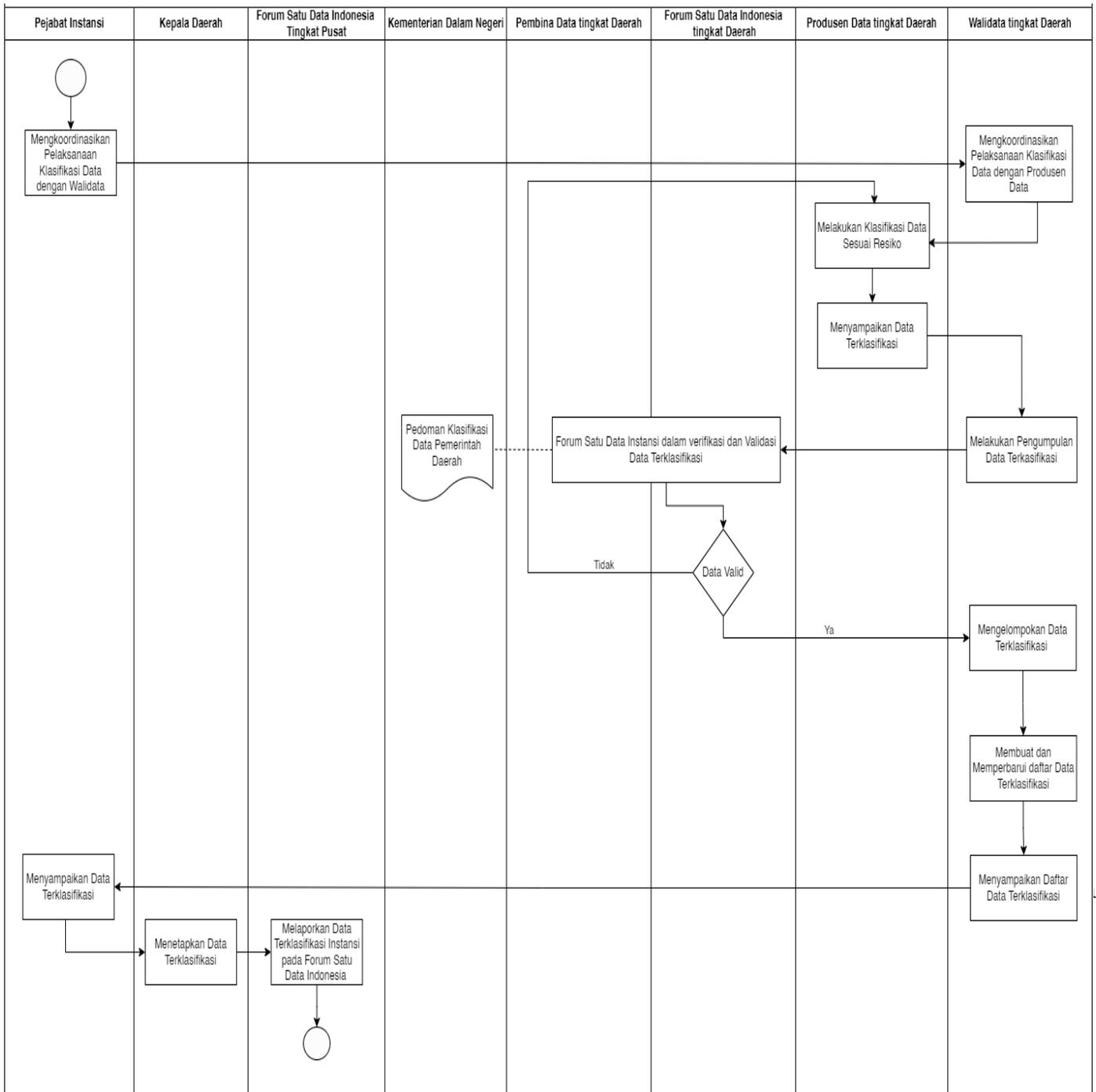


Gambar 2. Mekanisme Klasifikasi Data Sesuai Risiko PSE Lingkup Publik Pada Instansi Pusat

PELAKSANAAN KLASIFIKASI DATA PEMERINTAH DAERAH

Mekanisme pelaksanaan Klasifikasi Data Sesuai Risiko PSE Lingkup Publik pada Pemerintah Daerah pada Gambar 3. sebagai berikut:

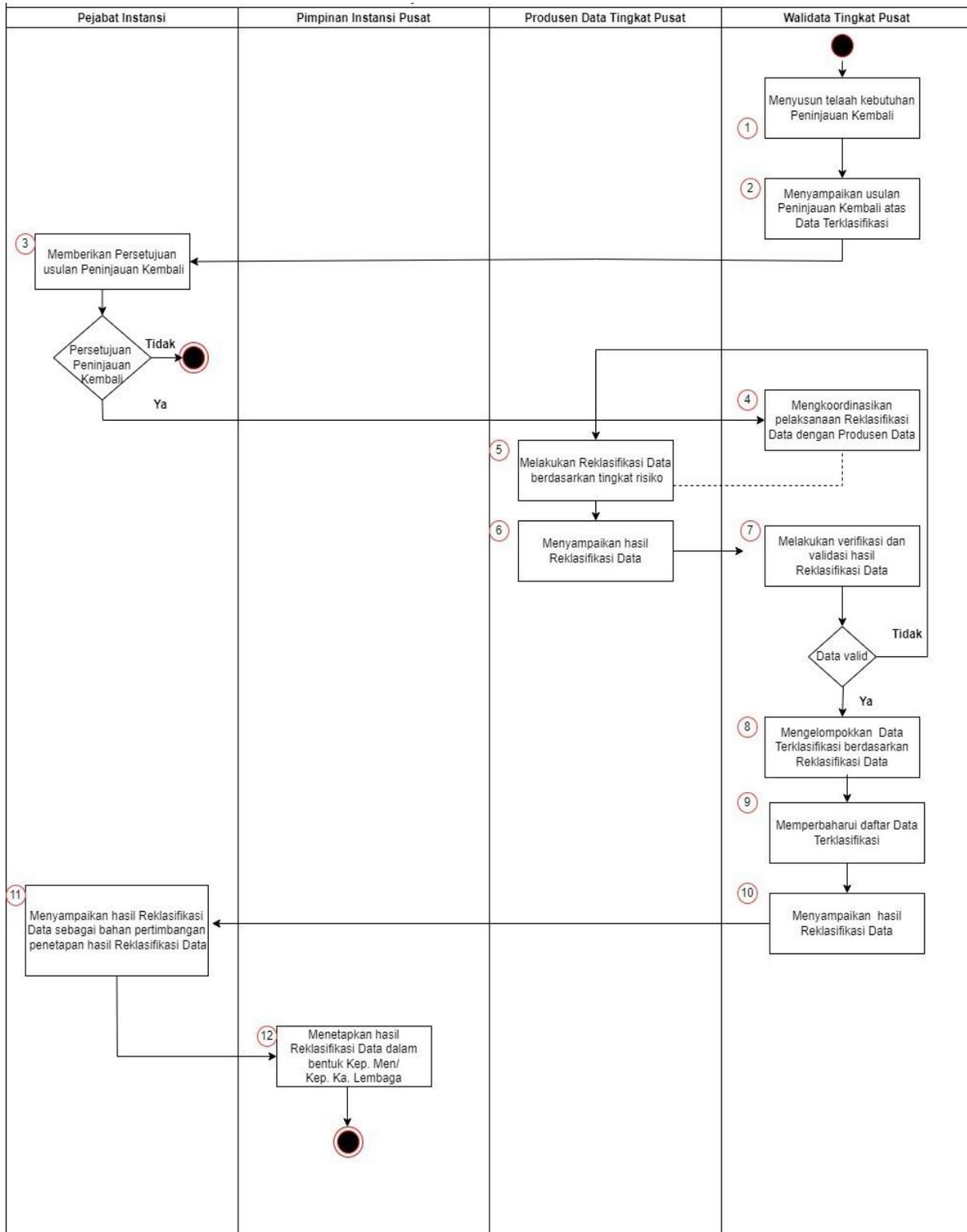
1. Pejabat Instansi mengoordinasikan pelaksanaan Klasifikasi Data Sesuai Risiko dengan Walidata tingkat daerah.
2. Walidata tingkat daerah berkoordinasi dengan Produsen Data tingkat daerah untuk melakukan Klasifikasi Data Sesuai Risiko.
3. Produsen Data tingkat daerah melakukan proses Klasifikasi Data Sesuai Risiko, sesuai dengan Tahapan Klasifikasi Data Sesuai Risiko, sebagai berikut:
 - a. penetapan area dampak risiko penyalahgunaan Data Elektronik
 - b. penetapan kriteria risiko penyalahgunaan Data Elektronik; dan
 - c. penentuan level risiko pada Klasifikasi Data Sesuai Risiko.
4. Produsen Data tingkat daerah menyampaikan Data Terklasifikasi kepada Walidata tingkat daerah.
5. Walidata tingkat daerah mengumpulkan Data Terklasifikasi dari Produsen Data tingkat daerah.
6. Walidata tingkat daerah bersama dengan Pembina Data tingkat daerah melakukan verifikasi dan validasi Data Terklasifikasi sesuai dengan mekanisme penilaian risiko yang disepakati dalam Forum Satu Data tingkat daerah. Apabila Data tidak valid maka Walidata tingkat daerah mengembalikan Data Terklasifikasi kepada Produsen Data tingkat daerah untuk dilakukan klasifikasi ulang.
7. Walidata tingkat daerah melakukan pengecekan kesesuaian proses klasifikasi datanya dengan pedoman klasifikasi data Pemerintah Daerah.
8. Apabila berdasarkan verifikasi dan validasi Data Terklasifikasi valid, Walidata tingkat daerah mengelompokkan Data sesuai kelompok Data Terklasifikasi.
9. Walidata tingkat daerah membuat dan memperbarui daftar Data Terklasifikasi.
10. Walidata tingkat daerah menyampaikan daftar Data Terklasifikasi kepada Pejabat Instansi.
11. Pejabat Instansi menyampaikan Data Terklasifikasi ke kepala daerah sebagai bahan pertimbangan penetapan Data Terklasifikasi.
12. Kepala Daerah menetapkan Data Terklasifikasi dalam bentuk keputusan kepala daerah yang meliputi keputusan gubernur, keputusan walikota, atau keputusan bupati.
13. Hasil Data Terklasifikasi yang telah ditetapkan oleh kepala daerah dilaporkan kepada Forum Satu Data Indonesia tingkat pusat.



PELAKSANAAN PENINJAUAN KEMBALI DAN REKLASIFIKASI DATA INSTANSI PUSAT

Mekanisme pelaksanaan Peninjauan Kembali dan Reklasifikasi Data PSE Lingkup Publik pada Instansi Pusat pada Gambar 4. sebagai berikut:

1. Walidata tingkat pusat menyusun telaah kebutuhan Peninjauan Kembali, yang meliputi:
 - a. penilaian ulang tingkat risiko;
 - b. hasil pemantauan dan evaluasi penyelenggaraan Klasifikasi Data Sesuai Risiko;
 - c. perubahan kebijakan nasional; dan/atau
 - d. perubahan proses bisnis;
2. Walidata tingkat pusat menyampaikan usulan Peninjauan Kembali atas Data Terklasifikasi kepada Pejabat Instansi.
3. Pejabat Instansi memberikan persetujuan atas usulan Peninjauan Kembali, dengan alternatif:
 - a. apabila usulan tidak disetujui maka proses Peninjauan Kembali tidak dilanjutkan.
 - b. apabila usulan disetujui, maka proses usulan Peninjauan Kembali dapat dilanjutkan dengan melakukan Reklasifikasi Data. Pejabat Instansi menyampaikan persetujuan kepada Walidata tingkat pusat.
4. Walidata tingkat pusat berkoordinasi dengan Produsen Data tingkat pusat untuk melakukan Reklasifikasi Data.
5. Produsen Data tingkat pusat melakukan Reklasifikasi Data berdasarkan pengukuran besaran nilai risiko dan penetapan tingkat risiko.
6. Hasil Reklasifikasi Data yang telah dilakukan oleh Produsen Data tingkat pusat disampaikan kepada Walidata tingkat pusat.
7. Walidata tingkat pusat melakukan verifikasi dan validasi atas hasil Reklasifikasi Data yang dilakukan oleh Produsen Data tingkat pusat. Apabila Data tidak valid, maka Walidata tingkat pusat mengembalikan hasil Reklasifikasi Data kepada Produsen Data tingkat pusat untuk dilakukan reklasifikasi ulang.
8. Berdasarkan hasil verifikasi dan validasi Data Terklasifikasi valid, Walidata tingkat pusat mengelompokkan Data Terklasifikasi berdasarkan Reklasifikasi Data.
9. Walidata tingkat pusat memperbaharui daftar Data Terklasifikasi.
10. Walidata tingkat pusat menyampaikan hasil Reklasifikasi Data kepada Pejabat Instansi.
11. Pejabat Instansi menyampaikan hasil Reklasifikasi Data kepada pimpinan Instansi Pusat sebagai bahan pertimbangan penetapan hasil Reklasifikasi Data.
12. Pimpinan Instansi Pusat menetapkan hasil Reklasifikasi Data dalam bentuk keputusan menteri atau keputusan lembaga.

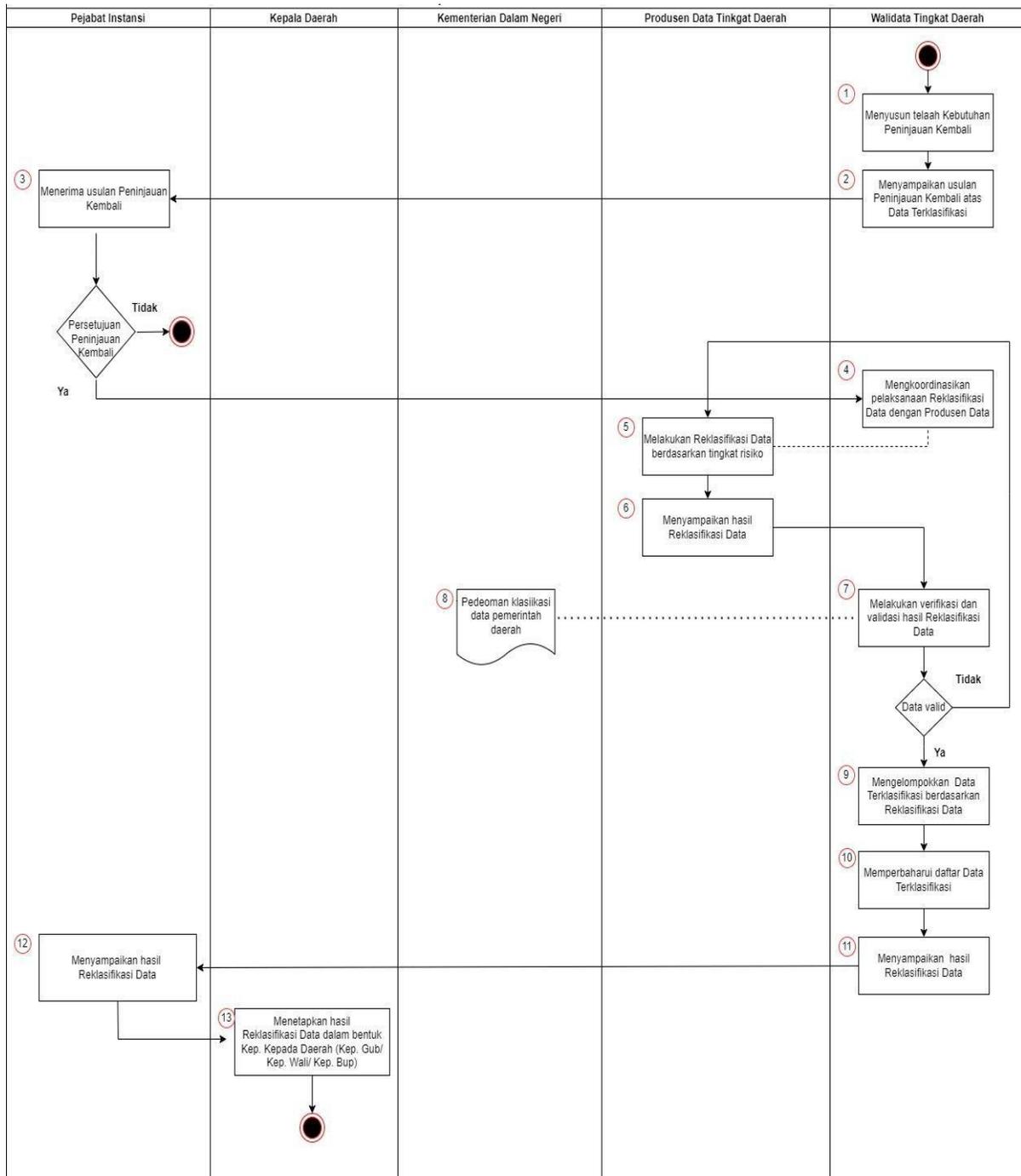


Gambar 4. Mekanisme Peninjauan Kembali dan Reklasifikasi Data pada Instansi Pusat

PELAKSANAAN PENINJAUAN KEMBALI DAN REKLASIFIKASI DATA
PEMERINTAH DAERAH

Mekanisme pelaksanaan Peninjauan Kembali dan Reklasifikasi Data PSE Lingkup Publik pada Pemerintah Daerah pada Gambar 5. sebagai berikut:

1. Walidata tingkat daerah menyusun telaah kebutuhan Peninjauan Kembali, yang meliputi:
 - a. penilaian ulang tingkat risiko;
 - b. hasil pemantauan dan evaluasi penyelenggaraan Klasifikasi Data Sesuai Risiko;
 - c. perubahan kebijakan nasional; dan/atau
 - d. perubahan proses bisnis.
2. Walidata tingkat daerah menyampaikan usulan Peninjauan Kembali atas Data Terklasifikasi kepada Pejabat Instansi.
3. Pejabat Instansi memberikan persetujuan atas usulan Peninjauan Kembali, dengan alternatif:
 - a. apabila usulan tidak disetujui maka proses Peninjauan Kembali tidak dilanjutkan.
 - b. apabila usulan disetujui, maka proses usulan Peninjauan Kembali dapat dilanjutkan dengan melakukan Reklasifikasi Data. Pejabat Instansi menyampaikan persetujuan kepada Walidata tingkat daerah.
4. Berdasarkan persetujuan Pejabat Instansi, Walidata tingkat daerah berkoordinasi dengan Produsen Data tingkat daerah untuk melakukan Reklasifikasi Data.
5. Produsen Data tingkat daerah melakukan proses Reklasifikasi Data berdasarkan pengukuran besaran nilai risiko dan penetapan tingkat risiko.
6. Produsen Data tingkat daerah menyampaikan hasil proses Reklasifikasi Data kepada Walidata tingkat daerah.
7. Walidata tingkat daerah melakukan verifikasi dan validasi atas hasil Reklasifikasi Data yang dilakukan oleh Produsen Data tingkat daerah. Apabila Data tidak valid maka Walidata tingkat daerah mengembalikan hasil Reklasifikasi Data kepada Produsen Data tingkat daerah untuk dilakukan reklasifikasi ulang.
8. Walidata tingkat daerah melakukan pengecekan kesesuaian proses klasifikasi datanya dengan pedoman klasifikasi data Pemerintah Daerah.
9. Berdasarkan hasil verifikasi dan validasi Data Terklasifikasi valid, Walidata tingkat daerah mengelompokkan Data Terklasifikasi berdasarkan Reklasifikasi Data.
10. Walidata tingkat daerah memperbaharui daftar Data Terklasifikasi
11. Walidata tingkat daerah menyampaikan hasil Reklasifikasi Data kepada Pejabat Instansi.
12. Pejabat Instansi menyampaikan hasil Reklasifikasi Data kepada kepala daerah sebagai bahan pertimbangan penetapan hasil Reklasifikasi Data.
13. Kepala daerah menetapkan hasil Reklasifikasi Data dalam bentuk keputusan kepala daerah yang meliputi keputusan gubernur, keputusan walikota, atau keputusan bupati.



Gambar 5. Mekanisme Peninjauan Kembali dan Reklasifikasi Data pada Pemerintah Daerah

MENTERI KOMUNIKASI DAN DIGITAL
REPUBLIC INDONESIA,

ttd

MEUTYA VIADA HAFID