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]

xxxxx

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	PIHAK KEDUA
Materai dan Ttd	Ttd
.....	.....
NIP.....	NIP...

Catatan : Asli dibuat dua rangkap, rangkap kedua Materai 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	Format: 1. Karakter nama [Lembaga Tinggi Negara].go.id 2. Karakter nama [Sekretariat Jenderal]. [Lembaga Tinggi Negara].go.id Contoh: a. DPR RI: dpr.go.id b. Sekretariat Jenderal DPR RI: setjen.dpr.go.id (sebagai contoh subdomain untuk membedakan penggunaan *email* antara anggota DPR dan jajaran staf di lingkungan kesekjenan DPR RI)
Legislatif Daerah dan Sekretariat Lembaga Legislatif Daerah	Format: 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 Contoh: a. DPRD Provinsi Kalteng: dprd-kaltengprov.go.id b. Sekretariat DPRD Provinsi Kalteng : sekretariat.dprd-kaltengprov.go.id c. (sebagai contoh subdomain untuk membedakan penggunaan *email* antara anggota DPRD dan jajaran staf di lingkungan kesekjenan DPRD). d. Dewan Perwakilan Rakyat Papua: dpr-papua.go.id e. Sekretariat DPR Papua : sekretariat.dpr-papua.go.id f. Dewan Perwakilan Rakyat Daerah Kabupaten Ponorogo : dprd-ponorogo.go.id g. Sekretariat DPRD Kabupaten Ponorogo : sekretariat.dprd-ponorogo.go.id

INSTANSI	FORMAT PENAMAAN NAMA DOMAIN
Kementerian	Format: Karakter nama [Kementerian].go.id Contoh: a. Kementerian Perindustrian: kemenperin.go.id b. Kementerian Komunikasi dan Digital: komdigi.go.id
Lembaga Setingkat Kementerian, Instansi vertikalnya di daerah, dan instansi kewilayahan di daerah	Format: 1. Karakter nama [Lembaga setingkat Kementerian].go.id 2. Karakter nama [(Singkatan)Lembaga Setingkat Kementerian – Lokasi Keberadaan Lembaga yang dimaksud].go.id Contoh: a. Kejaksaan Agung RI: kejaksaan.go.id b. Kejaksaan Tinggi Prov DIY: kejati-diy.go.id c. Kejaksaan Negeri Kota Bekasi: kejari-bekasikota.go.id d. Pengadilan Tinggi Tata Usaha Negara Medan: pttun-medan.go.id e. Pengadilan Tinggi Agama Banjarmasin : pta-banjarmasin.go.id f. Pengadilan Agama Kota Depok: pa-depok.go.id
Instansi Pemerintah Non-Kementerian dan instansi lainnya yang dibentuk peraturan perundang-undangan	Format: Karakter nama [Instansi pemerintah non kementerian].go.id Contoh: a. Badan Pusat Statistik: bps.go.id b. Badan Pembinaan Ideologi Pancasila: bpip.go.id c. Bank Indonesia: bi.go.id

INSTANSI	FORMAT PENAMAAN NAMA DOMAIN
Komisi, Badan, lembaga, atau instansi yang dibentuk berdasarkan peraturan perundang undangan dan atau dibiayai oleh Negara, dan Sekretariatnya;	Format: 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; Contoh: 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
Pemerintah Daerah	Format: 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 Contoh: 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
	Subdomain: Dinas Pendidikan Kabupaten Minahasa Tenggara: disdik.mitrakab.go.id Catatan: Selama tidak diidentifikasi atau tidak berpotensi diidentifikasikan duplikasi nama, maka diizinkan tidak menggunakan istilah prov, kab atau kota.

CONTOH NAMA DOMAIN PEMERINTAH DESA

INSTANSI	FORMAT PENAMAAN NAMA DOMAIN
Pemerintah Desa	Format: 1. Karakter nama [nama desa, atau singkatannya atau sebutan lain].desa.id 2. Karakter nama [nama desa, atau singkatannya]-[nama kabupaten/kota/kecamatan lokasi desa berada].desa.id Contoh: a. Desa Sukamaju Kabupaten Bogor: sukamaju-jonggol.desa.id b. Desa Sukamaju Kabupaten Bandung: sukamaju-majalaya.desa.id 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.

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: • layanan pengaduan publik: lapor.go.id • layanan perpajakan: pajak.go.id • layanan *National Single Window*: 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	Format: Karakter nama [Kegiatan Kenegaraan].go.id, atau Contoh: a. kegiatan untuk Pekan Olahraga Nasional: pon.go.id b. kegiatan Musabaqah Tilawatil Quran: musabaqah.go.id Catatan: Dalam hal kegiatan berskala nasional dan/atau Internasional dimaksud merupakan kegiatan internasional, Nama Domain dapat menggunakan bahasa asing

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	• Urusan pemerintahan sehari-hari, pemberian layanan, dan keuangan publik; • hubungan internasional rutin dan kegiatan diplomatik; • Keamanan publik, peradilan pidana dan kegiatan penegakan hukum;	• Keselamatan, keamanan atau kemakmuran Indonesia atau negara sahabat dengan mempengaruhi kepentingan finansial, ekonomi dan keuangan; • Keamanan dan ketahanan aset Infrastruktur Nasional yang penting;	• 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
	• Berefek pada aspek pertahanan, keamanan dan ketahanan; • Kepentingan finansial, termasuk informasi yang diberikan secara rahasia dan kekayaan intelektual	• 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.	Infrastruktur Nasional Penting yang signifikan; • 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.	• 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.	• 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 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.

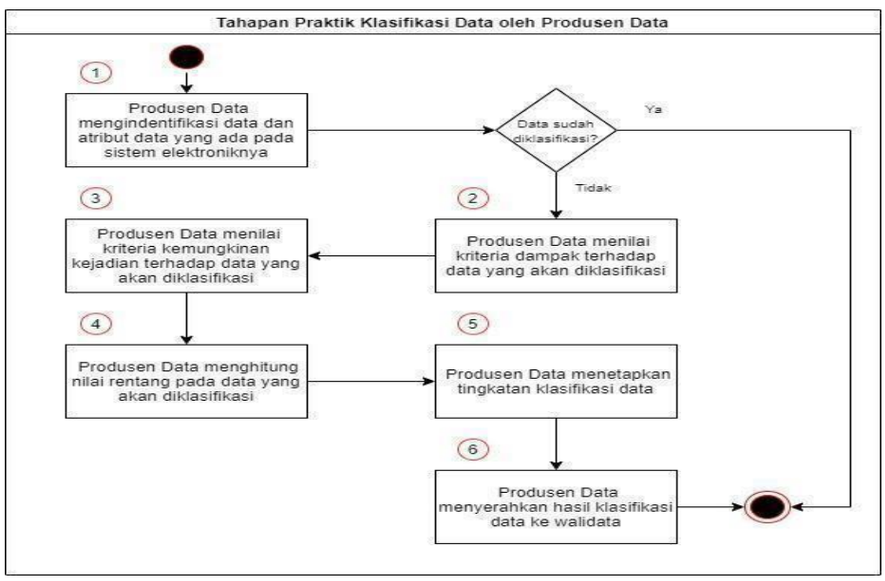
Pada Tabel 4 disampaikan nilai rentang klasifikasi data untuk 3 (tiga) kelompok. Hal ini ditujukan bagi Instansi tingkat pusat dan Pemerintah Daerah yang telah melakukan praktik Klasifikasi Data Sesuai Risiko dan menggunakan 3 (tiga) kelompok Data Terklasifikasi.

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 berbasiskan penilaian risiko, yaitu pada Gambar 1.



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

Tahapan praktik klasifikasi data oleh Produsen Data:

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	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: 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	1. Nama sistem senjata 2. Pengelola 3. Jumlah 4. Lokasi 5. penyimpanan 6. Kondisi	Kementerian Pertahanan	Kerahasiaan	Tinggi	5	15
				Integritas	Tinggi	5	
				Ketersediaan	Tinggi	5	
5	Daftar Fasilitas Kesehatan	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 Ruangan 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.

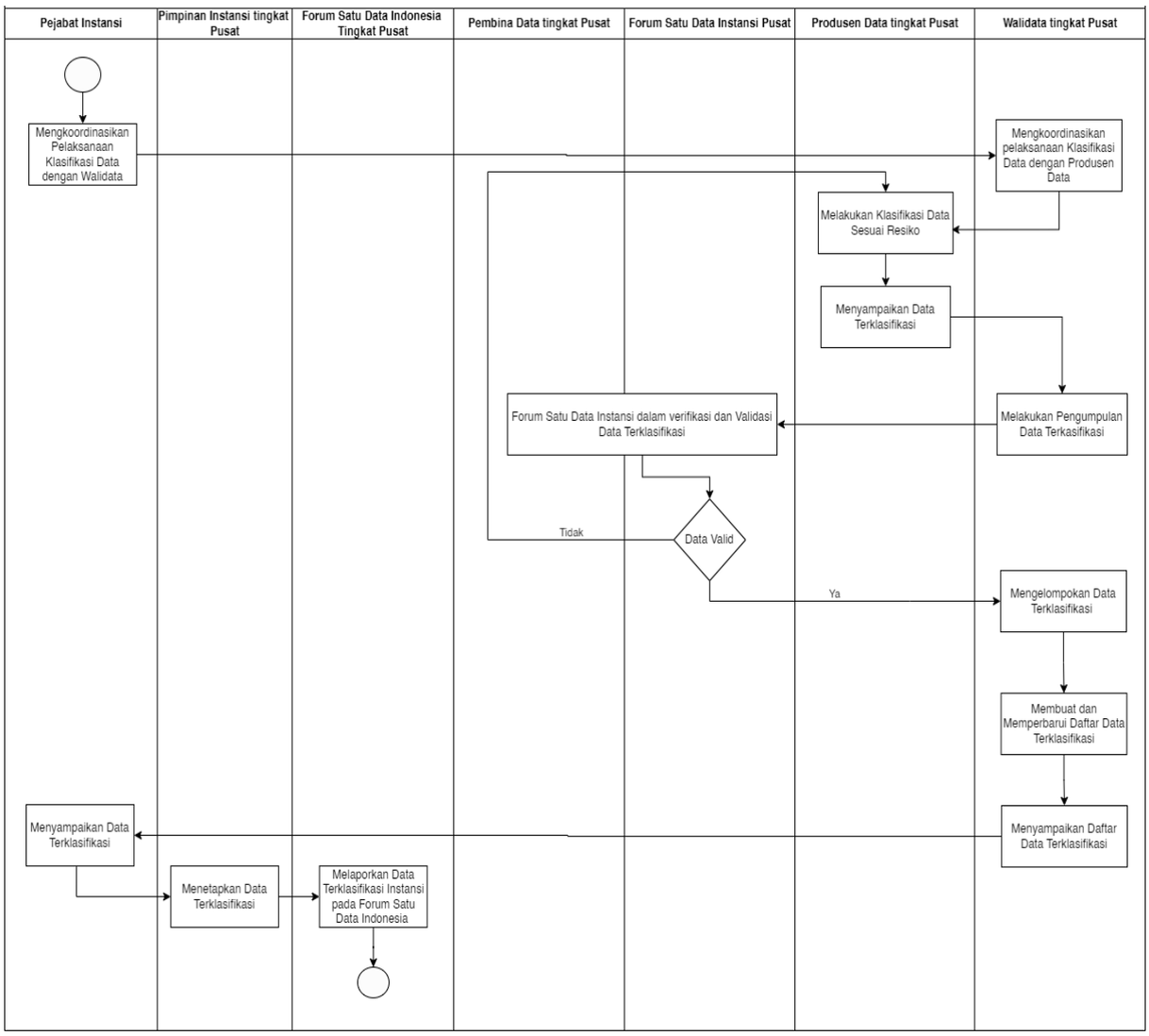
5. Menyerahkan hasil Klasifikasi Data Sesuai Risiko

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.

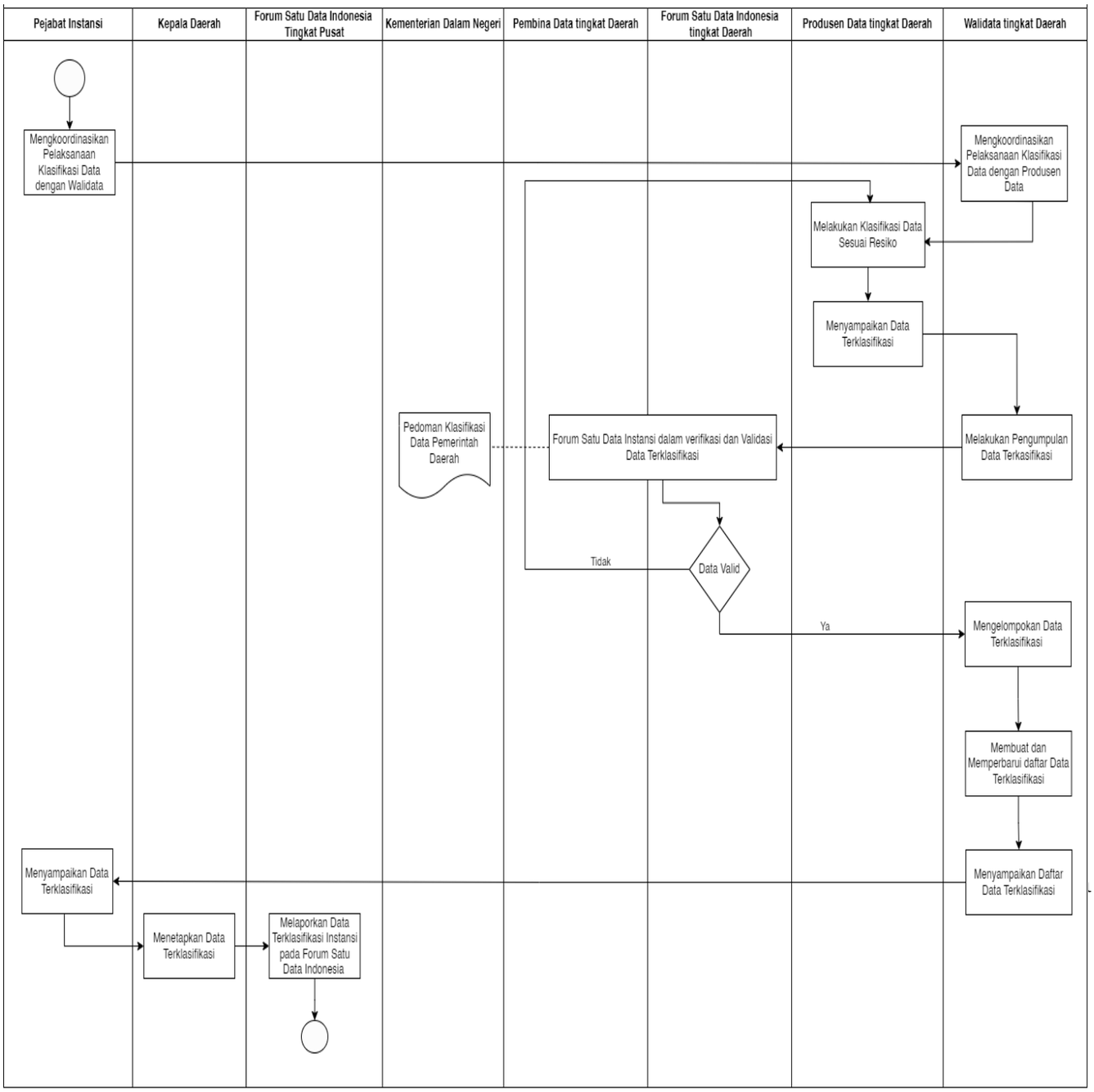


Gambar 2. Mekanisme Klasifikasi Data Sesuai Risiko PSE Lingkup Publik Pada Instansi Pusat

PELAKSANAAN KLASIFIKASI DATA PEMERINTAH DAERAH

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

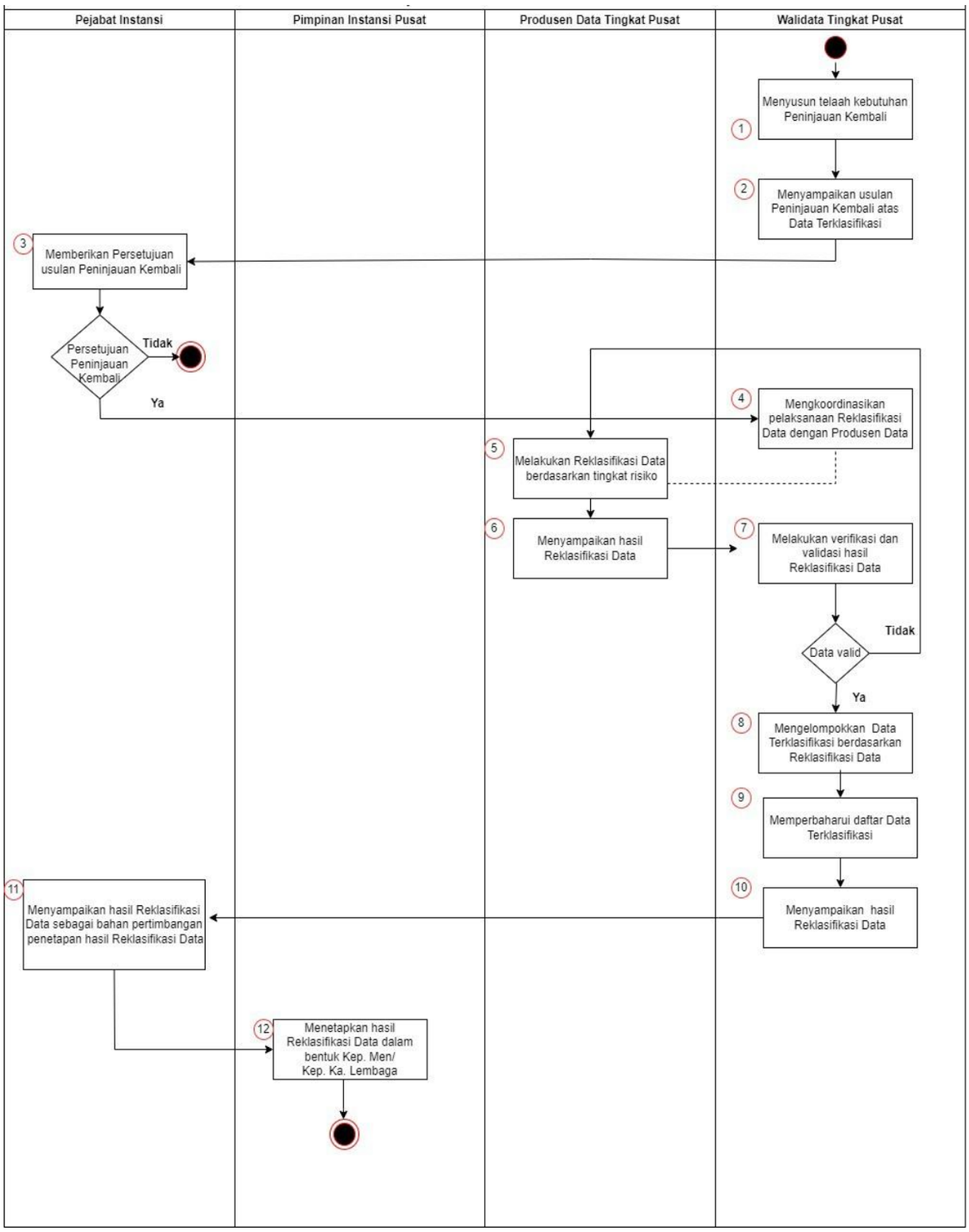
1. Pejabat Instansi mengoordinasikan pelaksanaan Klasifikasi Data Sesuai Risiko dengan Walidata tingkat daerah.
2. Walidata tingkat daerah berkoordinasi dengan Produsen Data tingkat daerah untuk melakukan Klasifikasi Data Sesuai Risiko.
3. Produsen Data tingkat daerah melakukan proses Klasifikasi Data 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.


Pejabat Instansi
Kepala Daerah
Forum Satu Data Indonesia Tingkat Pusat
Kementerian Dalam Negeri
Pembina Data tingkat Daerah
Forum Satu Data Indonesia tingkat Daerah
Produsen Data tingkat Daerah
Walidata tingkat Daerah
Mengkoordinasikan Pelaksanaan Klasifikasi Data dengan Walidata
Mengkoordinasikan Pelaksanaan Klasifikasi Data dengan Produsen Data
Melakukan Klasifikasi Data Sesuai Resiko
Menyampaikan Data Terklasifikasi
Pedoman Klasifikasi Data Pemerintah Daerah
Forum Satu Data Instansi dalam verifikasi dan Validasi Data Terklasifikasi
Melakukan Pengumpulan Data Terkasifikasi
Tidak
Data Valid
Ya
Mengelompokan Data Terklasifikasi
Membuat dan Memperbarui daftar Data Terklasifikasi
Menyampaikan Daftar Data Terklasifikasi
Menyampaikan Data Terklasifikasi
Menetapkan Data Terklasifikasi
Melaporkan Data Terklasifikasi Instansi pada Forum Satu Data Indonesia

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 Reklasfikasi Data kepada pimpinan Instansi Pusat sebagai bahan pertimbangan penetapan hasil Reklasfikasi Data.
12. Pimpinan Instansi Pusat menetapkan hasil Reklasifikasi Data dalam bentuk keputusan menteri atau keputusan lembaga.

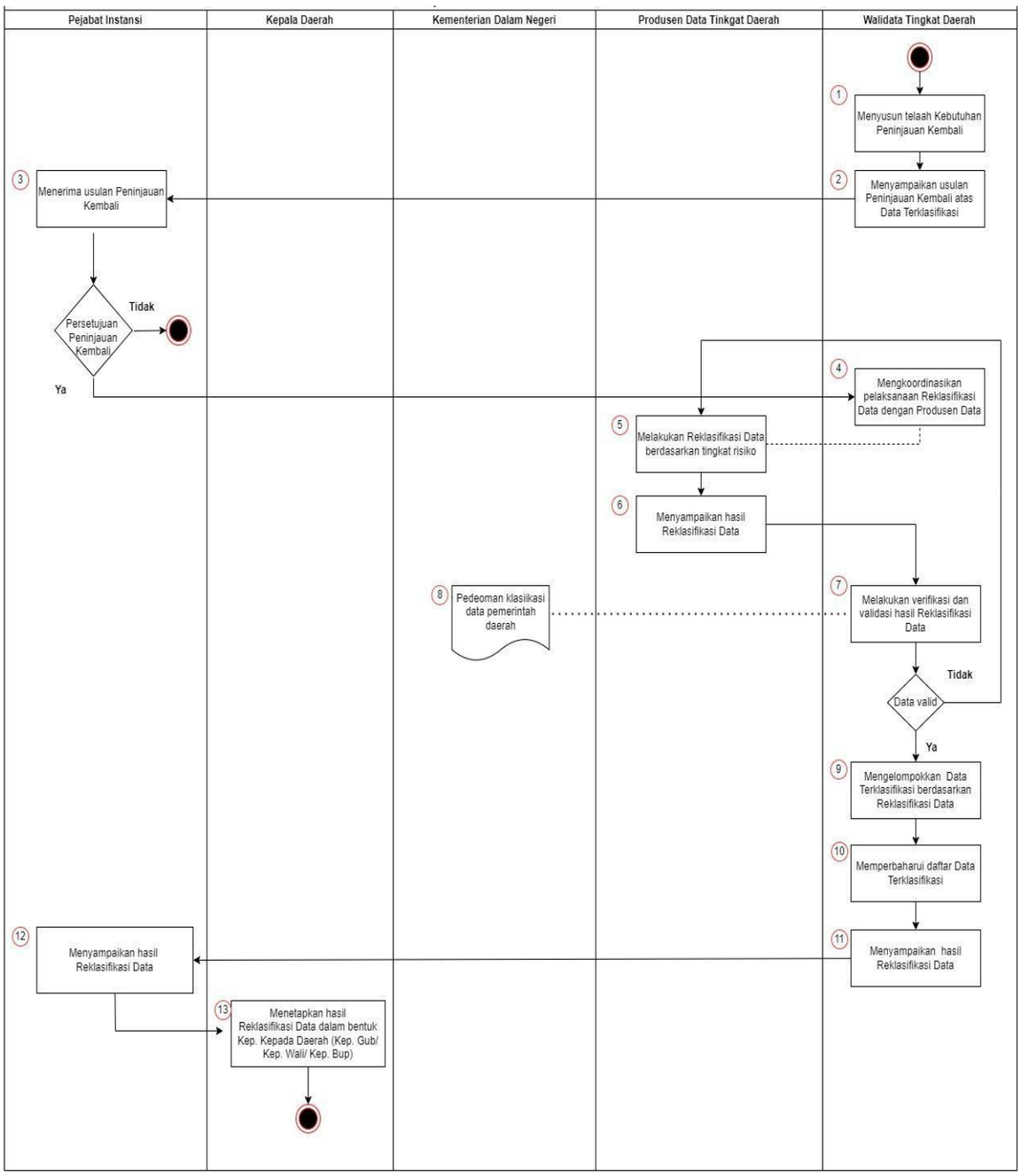


Gambar 4. Mekanisme Peninjauan Kembali dan Reklasifikasi Data pada Instansi Pusat

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 Reklasfikasi Data kepada kepala daerah sebagai bahan pertimbangan penetapan hasil Reklasfikasi 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
REPUBLIK INDONESIA,

ttd

MEUTYA VIADA HAFID