



PERATURAN MENTERI PERENCANAAN PEMBANGUNAN NASIONAL/
KEPALA BADAN PERENCANAAN PEMBANGUNAN NASIONAL
REPUBLIK INDONESIA
NOMOR 7 TAHUN 2025
TENTANG
PEDOMAN BERBAGIPAKAI
DATA TUNGGAL SOSIAL DAN EKONOMI NASIONAL

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PERENCANAAN PEMBANGUNAN NASIONAL/
KEPALA BADAN PERENCANAAN PEMBANGUNAN NASIONAL
REPUBLIK INDONESIA,

- Menimbang : a. bahwa untuk mendukung perencanaan program pembangunan kementerian, lembaga, dan pemerintah daerah, perlu memanfaatkan Data Tunggal Sosial dan Ekonomi Nasional;
- b. bahwa untuk mendukung keterpaduan program pembangunan nasional dan sinergi antar kementerian, lembaga, dan pemerintah daerah diperlukan pengelolaan Data Tunggal Sosial dan Ekonomi Nasional yang akurat dan terintegrasi;
- c. bahwa untuk melaksanakan pengelolaan Data Tunggal Sosial dan Ekonomi Nasional yang akurat dan terintegrasi, dibutuhkan pedoman berbagipakai Data Tunggal Sosial dan Ekonomi Nasional yang komprehensif;
- d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Menteri Perencanaan Pembangunan Nasional/Kepala Badan Perencanaan Pembangunan Nasional tentang Pedoman Berbagipakai Data Tunggal Sosial dan Ekonomi Nasional;
- Mengingat : 1. Pasal 17 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 25 Tahun 2004 tentang Sistem Perencanaan Pembangunan Nasional (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 104);
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 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196);
 5. 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 6905);
 6. Peraturan Pemerintah Nomor 40 Tahun 2006 tentang Tata Cara Penyusunan Rencana Pembangunan Nasional (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 97);
 7. Peraturan Pemerintah Nomor 17 Tahun 2017 tentang Sinkronisasi Proses Perencanaan dan Penganggaran Pembangunan Nasional (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 105);
 8. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185);
 9. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
 10. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
 11. Peraturan Presiden Nomor 132 Tahun 2022 Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 233);
 12. Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 159);
 13. Peraturan Presiden Nomor 194 Tahun 2024 tentang Kementerian Perencanaan Pembangunan Nasional (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 391);
 14. Peraturan Presiden Nomor 195 Tahun 2024 tentang Badan Perencanaan Pembangunan Nasional (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 392);
 15. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Pelindungan Data Pribadi dalam Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2016 Nomor 1829);
 16. Peraturan Menteri Perencanaan Pembangunan Nasional/Kepala Badan Perencanaan Pembangunan Nasional Nomor 5 Tahun 2018 tentang Tata Cara

Penyusunan Rencana Kerja Pemerintah (Berita Negara Nomor 2018 Nomor 408);

17. Peraturan Menteri Perencanaan Pembangunan Nasional/Kepala Badan Perencanaan Pembangunan Nasional Nomor 2 Tahun 2025 tentang Organisasi dan Tata Kerja Kementerian Perencanaan Pembangunan Nasional/Badan Perencanaan Pembangunan Nasional (Berita Negara Republik Indonesia Tahun 2025 Nomor 239);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI PERENCANAAN PEMBANGUNAN NASIONAL/KEPALA BADAN PERENCANAAN PEMBANGUNAN NASIONAL TENTANG PEDOMAN BERBAGIPAKAI DATA TUNGGAL SOSIAL DAN EKONOMI NASIONAL.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Satu Data Indonesia yang selanjutnya disingkat SDI adalah kebijakan tata kelola Data pemerintah untuk menghasilkan Data yang akurat, mutakhir, terpadu, dan dapat dipertanggungjawabkan, serta mudah diakses dan dibagipakaikan antar Instansi Pusat dan Instansi Daerah melalui pemenuhan Standar Data, Metadata, Interoperabilitas Data, dan menggunakan Kode Referensi dan Data Induk.
2. Data adalah catatan atas kumpulan fakta atau deskripsi berupa angka, karakter, simbol, gambar, peta, tanda, isyarat, tulisan, suara, dan/atau bunyi, yang merepresentasikan keadaan sebenarnya atau menunjukkan suatu ide, objek, kondisi, atau situasi.
3. 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.
4. Subjek Data Pribadi adalah orang perseorangan yang pada dirinya melekat Data pribadi.
5. Data Tunggal Sosial dan Ekonomi Nasional yang selanjutnya disingkat DTSEN adalah basis Data tunggal individu, dan/atau keluarga yang mencakup kondisi sosial, ekonomi dan peringkat kesejahteraan keluarga, yang dibentuk dari penggabungan Data registrasi sosial dan ekonomi, Data terpadu kesejahteraan sosial, dan Data pensasaran percepatan penghapusan kemiskinan ekstrem serta telah dipadankan dengan Data kependudukan dan dimutakhirkan secara berkala yang dikelola oleh lembaga pemerintah yang melaksanakan tugas pemerintahan di bidang statistik.

6. Pengendali DTSEN adalah pengendali Data pribadi sebagaimana diatur dalam peraturan perundang-undangan di bidang perlindungan Data pribadi, yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali atas pemrosesan DTSEN sesuai dengan prinsip dan kewajiban yang diatur dalam peraturan perundang-undangan yang berlaku.
7. Prosesor DTSEN adalah prosesor Data pribadi sebagaimana ketentuan peraturan perundang-undangan di bidang perlindungan Data pribadi yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan Data pribadi atas nama Pengendali DTSEN.
8. Pengguna DTSEN adalah instansi pusat, pemerintah daerah, badan usaha milik negara, dan pemangku kepentingan yang menggunakan dan memanfaatkan DTSEN
9. Portal Satu Data Indonesia yang selanjutnya disingkat Portal SDI adalah media bagipakai Data di tingkat nasional yang dapat diakses melalui pemanfaatan teknologi dan komunikasi.
10. Instansi Pusat adalah kementerian, lembaga pemerintah nonkementerian, kesekretariatan lembaga negara, kesekretariatan lembaga nonstruktural, dan lembaga pemerintah lainnya.
11. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
12. Walidata adalah unit pada Instansi Pusat dan Pemerintah Daerah yang melaksanakan kegiatan pengumpulan, pemeriksaan, dan pengelolaan Data yang disampaikan oleh Produsen Data, serta menyebarluaskan Data.
13. Pemangku Kepentingan adalah orang perseorangan, masyarakat, akademisi, organisasi profesi, lembaga negara, badan hukum publik, badan pengelola, badan usaha, organisasi masyarakat sipil, perguruan tinggi, pelaku industri, media massa, dan mitra pembangunan.
14. Interoperabilitas Data adalah kemampuan Data untuk dibagipakaikan antar sistem elektronik yang saling berinteraksi.
15. Hak Akses adalah hak yang diberikan oleh Pengendali DTSEN kepada Prosesor DTSEN untuk dapat mengakses basis DTSEN sesuai dengan layanan yang diberikan.
16. Menteri adalah Menteri Perencanaan Pembangunan Nasional/Kepala Badan Perencanaan Pembangunan Nasional.

BAB II PRINSIP, PEDOMAN, TUJUAN, DAN RUANG LINGKUP

Pasal 2

Penyelenggaraan berbagipakai DTSEN dilakukan berdasarkan prinsip SDI.

Pasal 3

- (1) Pengaturan mengenai pedoman berbagipakai DTSEN dalam Peraturan Menteri ini dilaksanakan sesuai dengan peraturan perundang-undangan di bidang perlindungan Data pribadi, sistem pemerintahan berbasis elektronik, dan penyelenggaraan sistem elektronik oleh penyelenggara sistem elektronik lingkup publik.
- (2) Pedoman berbagipakai DTSEN yang diatur dalam Peraturan Menteri ini merupakan dasar bagi Pengendali DTSEN dan Prosesor DTSEN dalam menyelenggarakan layanan pemanfaatan DTSEN.

Pasal 4

Pedoman berbagipakai DTSEN bertujuan untuk:

- a. menyediakan panduan yang jelas dan komprehensif bagi Instansi Pusat, Pemerintah Daerah, dan/atau Pemangku Kepentingan dalam proses berbagipakai DTSEN;
- b. mengantisipasi duplikasi Data yang dihasilkan oleh Pengendali DTSEN sesuai amanah regulasi yang ditunjuk untuk melakukan pemrosesan dan berbagipakai Data;
- c. memastikan pelaksanaan kewajiban pengendali DTSEN dan prosesor DTSEN, dasar pemrosesan, serta pelaksanaan prinsip-prinsip perlindungan Data pribadi dalam penyelenggaraan berbagipakai DTSEN guna meminimalkan risiko hukum, melindungi Data Pribadi, dan menjaga keamanan Data dalam proses berbagipakai DTSEN;
- d. mendorong peningkatan transparansi, kepercayaan, dan akuntabilitas dalam proses berbagipakai DTSEN;
- e. memastikan integrasi DTSEN antar Instansi Pusat dan Pemerintah Daerah dalam konteks sistem pemerintah berbasis elektronik dan SDI dengan meningkatkan efisiensi dan interoperabilitas antar instansi dalam berbagi Data untuk layanan publik yang lebih baik; dan
- f. mendorong standarisasi dan validasi Data dalam lingkup kebijakan SDI.

Pasal 5

Ruang lingkup dalam pedoman berbagipakai DTSEN meliputi:

- a. kaidah berbagipakai DTSEN;
- b. penyelenggara berbagipakai DTSEN;
- c. penyelenggaraan berbagipakai DTSEN;
- d. klasifikasi Data dan manajemen Hak Akses;

- e. layanan Pemanfaatan DTSEN; dan
- f. pemantauan dan evaluasi.

BAB III KAIDAH BERBAGIPAKAI DTSEN

Pasal 6

Berbagipakai DTSEN harus dilakukan berdasarkan kaidah sebagai berikut:

- a. keamanan;
- b. transparansi; dan
- c. kepatuhan hukum.

Pasal 7

- (1) Kaidah keamanan sebagaimana dimaksud dalam Pasal 6 huruf a bertujuan untuk melindungi kerahasiaan, keutuhan/integritas, ketersediaan, keaslian dan kenirsangkalan DTSEN.
- (2) Kaidah keamanan sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan standar yang diatur oleh badan yang melaksanakan tugas pemerintahan di bidang keamanan siber dan persandian dan peraturan perundang-undangan di bidang perlindungan Data pribadi.

Pasal 8

- (1) Kaidah transparansi sebagaimana dimaksud dalam Pasal 6 huruf b bertujuan untuk membangun kepercayaan antara Pengendali DTSEN dan/atau Prosesor DTSEN, Subjek Data Pribadi, dan pihak-pihak terkait lainnya.
- (2) Kaidah transparansi sebagaimana dimaksud pada ayat (1) harus memberikan informasi yang jelas, rinci, dan mudah dipahami kepada Subjek Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 9

Kaidah kepatuhan hukum sebagaimana dimaksud dalam Pasal 6 huruf c bertujuan untuk memastikan penyelenggaraan berbagipakai DTSEN dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 10

Ketentuan lebih lanjut mengenai kaidah berbagipakai DTSEN sebagaimana dimaksud dalam Pasal 6 sampai dengan Pasal 9 diatur dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Peraturan Menteri ini.

BAB IV PENYELENGGARA BERBAGIPAKAI DTSEN

Bagian Kesatu Umum

Pasal 11

Penyelenggara berbagipakai DTSEN terdiri atas:

- a. Pengendali DTSEN;
- b. Prosesor DTSEN; dan
- c. Pengguna DTSEN.

Bagian Kedua Pengendali DTSEN

Pasal 12

- (1) Pengendali DTSEN dalam menyelenggarakan berbagipakai DTSEN memiliki kewajiban sesuai dengan ketentuan peraturan perundang-undangan.
- (2) Pengendali DTSEN sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. kementerian yang menyelenggarakan urusan pemerintahan di bidang perencanaan pembangunan nasional;
 - b. kementerian yang menyelenggarakan sinkronisasi dan koordinasi serta pengendalian urusan kementerian dalam penyelenggaraan pemerintahan di bidang pemberdayaan masyarakat;
 - c. kementerian yang menyelenggarakan urusan pemerintahan di bidang sosial; dan
 - d. badan yang melaksanakan tugas pemerintahan di bidang statistik.
- (3) Pengendali DTSEN sebagaimana dimaksud pada ayat (2) bertindak dan bertanggung jawab sendiri-sendiri terhadap aktifitas penyelenggaraan DTSEN.
- (4) Pengendali DTSEN sebagaimana dimaksud pada ayat (2) melaksanakan bagipakai DTSEN sesuai dengan tugas dan fungsinya.
- (5) Menteri/kepala badan Pengendali DTSEN sebagaimana dimaksud pada ayat (2) menunjuk unit kerja dan/atau pejabat yang mewakili kementerian dan/atau badan sebagai Pengendali DTSEN dan petugas pelindung Data pribadi.
- (6) Penunjukan unit kerja dan/atau pejabat yang mewakili kementerian dan/atau badan sebagai Pengendali DTSEN dan petugas pelindung Data pribadi sebagaimana dimaksud pada ayat (5), ditetapkan melalui keputusan menteri dan/atau keputusan kepala badan sesuai kewenangannya.

Bagian Ketiga
Prosesor DTSEN

Pasal 13

- (1) Pengendali DTSEN sebagaimana dimaksud dalam Pasal 11 huruf a dapat menunjuk Prosesor DTSEN dalam melakukan pemrosesan DTSEN.
- (2) Pemrosesan DTSEN oleh Prosesor DTSEN sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan peraturan perundang-undangan di bidang perlindungan Data pribadi.

Bagian Keempat
Pengguna DTSEN

Pasal 14

- (1) Pengguna DTSEN dapat memanfaatkan DTSEN berdasarkan tugas dan kewenangan sesuai dengan ketentuan peraturan perundang-undangan.
- (2) Pemanfaatan DTSEN sebagaimana dimaksud pada ayat (1) dilakukan dengan mengajukan permohonan penggunaan DTSEN kepada Pengendali DTSEN dengan dilampiri dokumen.
- (3) Pengguna DTSEN sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. Walidata Instansi Pusat;
 - b. Walidata Pemerintah Daerah;
 - c. koordinator forum satu data Indonesia tingkat daerah;
 - d. unit kerja yang ditunjuk oleh menteri/kepala dan/atau perangkat daerah yang ditunjuk oleh kepala daerah; dan/atau
 - e. unit kerja yang menyelenggarakan tugas dan fungsi di bidang pengelolaan Data dan informasi di badan usaha milik negara.
- (4) Pengguna DTSEN sebagaimana dimaksud pada ayat (3) huruf e merupakan badan usaha milik negara yang diberikan tugas oleh pemerintah terkait program bantuan sosial, bantuan pemerintah, dan subsidi.
- (5) Pengguna DTSEN sebagaimana dimaksud pada ayat (3) menjadi Pengendali DTSEN atas DTSEN yang diterimanya.
- (6) Pengendali DTSEN sebagaimana dimaksud pada ayat (5) wajib melakukan perlindungan Data pribadi sesuai dengan peraturan perundang-undangan di bidang perlindungan Data pribadi.

Pasal 15

Ketentuan lebih lanjut mengenai penyelenggara DTSEN sebagaimana dimaksud dalam Pasal 11 sampai dengan Pasal 14 diatur dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Peraturan Menteri ini.

BAB V PENYELENGGARAAN BERBAGIPAKAI DTSEN

Bagian Kesatu Umum

Pasal 16

- (1) Penyelenggaraan berbagipakai DTSEN terdiri atas:
 - a. Pengajuan permintaan Data;
 - b. Pengecekan permintaan Data;
 - c. Pengiriman Data; dan
 - d. Pemanfaatan Data dan pelaporan.
- (2) Penyelenggaraan berbagipakai DTSEN sebagaimana dimaksud pada ayat (1) dilakukan melalui Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN.
- (3) Penyelenggaraan berbagipakai DTSEN sebagaimana dimaksud pada ayat (1) menggunakan fasilitas ekosistem pusat Data nasional, jaringan intra pemerintah, dan sistem penghubung layanan pemerintah.
- (4) Dalam hal jaringan intra pemerintah sebagaimana dimaksud pada ayat (3) belum tersedia, penyelenggaraan berbagipakai DTSEN tetap dilaksanakan dengan memastikan keamanan dalam berbagipakai Data sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kedua Pengajuan Permintaan Data

Pasal 17

- (1) Pengajuan permintaan Data sebagaimana dimaksud dalam Pasal 16 ayat (1) huruf a dilakukan oleh Pengguna DTSEN kepada Pengendali DTSEN.
- (2) Pengajuan permintaan Data yang diajukan Pemerintah Daerah dilakukan oleh Walidata Pemerintah Daerah dan/atau perangkat daerah.
- (3) Dalam mengajukan permintaan Data sebagaimana dimaksud pada ayat (2) harus berkoordinasi dengan koordinator forum SDI tingkat Daerah.
- (4) Pengajuan permintaan Data yang diajukan badan usaha milik negara, dilakukan oleh unit kerja yang menyelenggarakan tugas dan fungsi di bidang pengelolaan Data dan informasi.
- (5) Pengajuan permintaan Data sebagaimana dimaksud pada ayat (2) dengan melampirkan dokumen:
 - a. surat pengajuan Data yang ditandatangani Menteri/kepala lembaga/kepala daerah;
 - b. kerangka acuan kerja;
 - c. peraturan perundang-undangan sebagai dasar pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan penggunaan DTSEN;

- d. penetapan pembentukan kelembagaan tentang pelaksana pengelolaan pemanfaatan DTSEN di tingkat kementerian/lembaga/pemerintah daerah;
 - e. Peraturan Menteri/kepala lembaga/kepala badan/kepala daerah tentang SDI; dan
 - f. dokumen pendukung lainnya.
- (6) Pengajuan permintaan Data sebagaimana dimaksud pada ayat (4) dengan melampirkan dokumen:
- a. surat permohonan Data yang ditandatangani kepala badan usaha milik negara;
 - b. kerangka acuan kerja;
 - c. peraturan perundang-undangan sebagai dasar pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan penggunaan DTSEN;
 - d. penetapan pembentukan kelembagaan tentang pelaksana pengelolaan pemanfaatan DTSEN;
 - e. keputusan kepala badan usaha milik negara yang menunjuk unit kerja yang menyelenggarakan tugas dan fungsi di bidang pengelolaan data dan informasi yang diberikan tugas oleh pemerintah terkait program bantuan sosial, bantuan pemerintah, dan subsidi; dan
 - f. dokumen pendukung lainnya.

Bagian Ketiga Pengecekan Permintaan Data

Pasal 18

- (1) Pengecekan permintaan Data sebagaimana dimaksud dalam Pasal 16 ayat (1) huruf b dilakukan oleh Pengendali DTSEN sebagaimana dimaksud dalam Pasal 12 ayat (2).
- (2) Pengecekan permintaan Data sebagaimana dimaksud pada ayat (1) dilakukan dengan verifikasi dan validasi terhadap kelengkapan, kesesuaian, keakuratan, dan keabsahan dokumen.
- (3) Hasil pengecekan permintaan Data sebagaimana dimaksud pada ayat (2) digunakan sebagai rekomendasi oleh Pengendali DTSEN untuk memberikan persetujuan atau penolakan atas permintaan data.

Bagian Keempat Pengiriman Data

Pasal 19

- (1) Pengiriman Data sebagaimana dimaksud dalam Pasal 16 ayat (1) huruf c dilakukan oleh Pengendali DTSEN sebagaimana dimaksud dalam Pasal 12 ayat (2) kepada Pengguna DTSEN.
- (2) Pengiriman Data sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan persetujuan permintaan data sebagaimana dimaksud dalam Pasal 18 ayat (3).

- (3) Pengiriman Data sebagaimana dimaksud pada ayat (1) dapat disertai dengan berita acara serah terima.
- (4) Berita acara serah terima sebagaimana dimaksud pada ayat (3) dapat memuat klausul perjanjian kerahasiaan (*non disclosure agreement*) sesuai dengan peraturan perundang-undangan di bidang perlindungan Data pribadi.
- (5) Pengguna DTSEN sebagaimana dimaksud pada ayat (1) tidak dapat membagikan DTSEN kepada pihak lainnya di luar kerangka kegiatan yang diusulkan dalam usulan pemanfaatan Data.
- (6) Dalam pengiriman Data sebagaimana dimaksud pada ayat (1) dilakukan melalui Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN sebagaimana dimaksud dalam Pasal 12 ayat (2) dengan mekanisme integrasi antar sistem (*Application Programming Interface Service*) dengan memanfaatkan sistem penghubung layanan pemerintah sesuai dengan ketentuan peraturan perundang-undangan.
- (7) Proses Integrasi sebagaimana dimaksud pada ayat (6) dilaksanakan dengan mempertimbangkan aspek keamanan Data dan informasi sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima Pemanfaatan Data dan Pelaporan

Pasal 20

- (1) Pemanfaatan Data dan pelaporan sebagaimana dimaksud dalam Pasal 16 ayat (1) huruf d dilakukan oleh Pengguna DTSEN dan Pengendali DTSEN.
- (2) Pengendali DTSEN dan Pengguna DTSEN dalam memanfaatkan DTSEN wajib menjaga keamanan Data berdasarkan standar yang diatur oleh badan yang melaksanakan tugas pemerintahan di bidang keamanan siber dan persandian dan peraturan perundang-undangan di bidang perlindungan Data pribadi.
- (3) Pengguna DTSEN yang memanfaatkan DTSEN sebagai pelaksanaan tugas dan fungsi, harus melaporkan pemanfaatan tersebut kepada Pengendali DTSEN sebagaimana dimaksud dalam Pasal 12 ayat (2) baik secara periodik atau sewaktu-waktu jika dibutuhkan.

Pasal 21

Ketentuan lebih lanjut mengenai penyelenggaraan berbagipakai DTSEN sebagaimana dimaksud dalam Pasal 16 sampai dengan Pasal 20 diatur dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Peraturan Menteri ini.

BAB VI KLASIFIKASI DAN MANAJEMEN HAK AKSES DTSEN

Pasal 22

- (1) Klasifikasi DTSEN terdiri atas:
 - a. Data terbuka;
 - b. Data terbatas; dan
 - c. Data tertutup.
- (2) Klasifikasi DTSEN sebagaimana dimaksud pada ayat (1) dilakukan oleh Pengendali DTSEN sesuai dengan ketentuan peraturan perundangan yang mengatur mengenai penyelenggaraan sistem elektronik oleh penyelenggara sistem elektronik lingkup publik.
- (3) Klasifikasi DTSEN sebagaimana dimaksud pada ayat (1) diatur dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Peraturan Menteri ini.

Pasal 23

- (1) Manajemen Hak Akses Data dalam pemanfaatan DTSEN dilaksanakan sesuai dengan Klasifikasi DTSEN sebagaimana dimaksud dalam Pasal 22.
- (2) Pengendali DTSEN sebagaimana dimaksud dalam Pasal 12 ayat (2) menetapkan manajemen Hak Akses Data dalam pemanfaatan DTSEN.

BAB VII LAYANAN PEMANFAATAN DATA TUNGGAL SOSIAL EKONOMI DAN NASIONAL

Pasal 24

- (1) Dalam rangka mendukung pemanfaatan DTSEN diperlukan Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN sebagaimana dimaksud dalam Pasal 12 ayat (2) sebagai media bagipakai DTSEN di tingkat nasional.
- (2) Pemanfaatan DTSEN yang dilakukan melalui Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN sebagaimana dimaksud pada ayat (1) disebut sebagai layanan pemanfaatan DTSEN.
- (3) Layanan pemanfaatan DTSEN sebagaimana dimaksud pada ayat (2) menyediakan Data berkualitas terintegrasi sebagai sumber Data utama dalam perencanaan, pelaksanaan, dan evaluasi kebijakan sosial dan ekonomi untuk memastikan program pemerintah terlaksana secara tepat sasaran, efektif, efisien, dan akuntabel.
- (4) Layanan pemanfaatan DTSEN sebagaimana dimaksud pada ayat (3) memiliki Hak Akses yang terdiri atas:
 - a. layanan pemanfaatan DTSEN agregat terbuka sebagai level 1 (satu) yang dapat diakses oleh Pengguna DTSEN dan Pemangku Kepentingan;
 - b. layanan pemanfaatan DTSEN kustomisasi sebagai level 2 (dua) yang dapat diakses oleh Pengguna DTSEN;

- c. layanan pemanfaatan DTSEN mikro sebagai level 3 (tiga) yang dapat diakses oleh Pengguna DTSEN; dan
 - d. layanan pemanfaatan DTSEN berdasarkan nama dan alamat sebagai level 4 (empat) yang dapat diakses oleh Pengguna DTSEN.
- (5) Dalam rangka meningkatkan kualitas layanan pemanfaatan DTSEN, Pengguna DTSEN dapat melakukan analisis dan pemanfaatan DTSEN hasil analisis melalui Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN sebagaimana dimaksud dalam Pasal 12 ayat (2) sesuai kebutuhan.

Pasal 25

Seluruh DTSEN yang telah dilakukan pemadanan dan pemutakhiran oleh badan yang melaksanakan tugas pemerintahan di bidang statistik, diserahkan kepada kementerian yang menyelenggarakan urusan pemerintahan di bidang sosial, kementerian yang menyelenggarakan sinkronisasi dan koordinasi serta pengendalian urusan kementerian dalam penyelenggaraan pemerintahan di bidang pemberdayaan masyarakat, dan kementerian yang menyelenggarakan urusan pemerintahan di bidang perencanaan pembangunan nasional.

Pasal 26

Standar Layanan yang dapat disediakan melalui Layanan Pemanfaatan DTSEN tercantum dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Peraturan Menteri ini.

BAB VIII

PEMANTAUAN DAN EVALUASI

Pasal 27

- (1) Pemantauan dan evaluasi dilakukan secara bersama atau sendiri-sendiri oleh:
 - a. kementerian yang menyelenggarakan urusan pemerintahan di bidang perencanaan pembangunan nasional; dan
 - b. kementerian yang menyelenggarakan sinkronisasi dan koordinasi serta pengendalian urusan kementerian dalam penyelenggaraan pemerintahan di bidang pemberdayaan masyarakat.
- (2) Kementerian sebagaimana dimaksud pada ayat (1), mempunyai tugas yaitu:
 - a. melakukan pengendalian berkala terhadap pengelolaan DTSEN;
 - b. memastikan aktivitas pemrosesan DTSEN dilakukan sesuai dengan ketentuan peraturan perundang-undangan;
 - c. melakukan evaluasi dampak pemanfaatan DTSEN; dan

- d. memastikan Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN sebagaimana dimaksud dalam Pasal 12 ayat (2) sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.
- (3) Kementerian sebagaimana dimaksud pada ayat (1) melakukan pemantauan dan evaluasi secara berkala paling sedikit 1 (satu) kali dalam setahun dan sewaktu-waktu apabila diperlukan.
- (4) Menteri pada kementerian sebagaimana dimaksud pada ayat (1) melaporkan hasil pemantauan dan evaluasi kepada Presiden.
- (5) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB IX KETENTUAN PERALIHAN

Pasal 28

- (1) Pengguna DTSEN yang belum memiliki kesiapan secara portal dan/atau sistem informasi dan/atau instrumen hukum sebagaimana dimaksud dalam Pasal 17 ayat (5) huruf e dalam melakukan bagipakai DTSEN sebagaimana dimaksud dalam Pasal 19 dapat menggunakan surat penunjukan Pengendali DTSEN.
- (2) Pengguna DTSEN sebagaimana dimaksud pada ayat (1) memiliki kewajiban untuk melakukan perlindungan Data pribadi sesuai dengan ketentuan peraturan perundang-undangan mengenai perlindungan Data pribadi.
- (3) Pengguna DTSEN yang belum memiliki kesiapan secara portal dan/atau sistem informasi sebagaimana dimaksud pada ayat (1), proses pengiriman Data dapat dilakukan melalui saluran yang terenkripsi dan terkunci, dengan akses yang hanya dapat dibuka berdasarkan autentikasi multifaktor dan/atau sertifikat elektronik sesuai standar keamanan informasi yang berlaku.
- (4) Pengguna DTSEN yang belum memiliki dasar hukum pemrosesan sebagaimana dimaksud dalam Pasal 17 ayat (5) huruf e, pada saat Peraturan Menteri ini diundangkan, pengiriman DTSEN pertama kali dapat dilakukan tanpa pemenuhan dokumen sebagaimana dimaksud dalam Pasal 17 ayat (5) huruf e.
- (5) Pengguna DTSEN sebagaimana dimaksud pada ayat (4) harus memiliki dasar hukum pemrosesan sebagaimana dimaksud dalam Pasal 17 ayat (5) huruf e paling lama 6 (enam) bulan terhitung sejak tanggal penerimaan DTSEN pertama kali.
- (6) Dalam jangka waktu paling lama 1 (satu) tahun sejak Peraturan Menteri ini diundangkan, Pengendali DTSEN dan Pengguna DTSEN yang belum memiliki sistem atau portal sebagaimana dimaksud dalam Pasal 16 ayat (2) harus memiliki portal atau sistem informasi.

BAB X
KETENTUAN PENUTUP

Pasal 29

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

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



Ditetapkan di Jakarta
pada tanggal 4 Agustus 2025

MENTERI PERENCANAAN
PEMBANGUNAN NASIONAL/
KEPALA BADAN
PERENCANAAN
PEMBANGUNAN NASIONAL
REPUBLIK INDONESIA,

RACHMAT PAMBUDY

Diundangkan di Jakarta
pada tanggal

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM REPUBLIK INDONESIA,

DHAHANA PUTRA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2025 NOMOR



LAMPIRAN
PERATURAN MENTERI
PERENCANAAN PEMBANGUNAN
NASIONAL/KEPALA BADAN
PERENCANAAN PEMBANGUNAN
NASIONAL NOMOR 7 TAHUN 2025
TENTANG PEDOMAN
BERBAGIPAKAI DATA TUNGGAL
SOSIAL DAN EKONOMI NASIONAL

PEDOMAN BERBAGIPAKAI
DATA TUNGGAL SOSIAL DAN EKONOMI NASIONAL

BAB I KAIDAH BERBAGIPAKAI DATA TUNGGAL SOSIAL DAN EKONOMI NASIONAL

Pemrosesan Data Tunggal Sosial dan Ekonomi Nasional (DTSEN) harus dilakukan dengan memperhatikan kaidah yang memastikan prinsip keamanan, transparansi, dan kepatuhan hukum dalam penggunaannya. Setiap pemrosesan harus dilakukan secara terbatas dan spesifik sesuai dengan kebutuhan yang sah secara hukum, serta dilakukan dengan prinsip keterbukaan agar dapat dipertanggungjawabkan, hal ini sejalan dengan prinsip Pasal 16 ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) serta Standar Keamanan Data dan Informasi berdasarkan Pasal 19 sampai dengan Pasal 24 Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, berikut beberapa kaidah yang harus dipenuhi oleh Pengguna DTSEN:

A. Keamanan

Menerapkan Standar teknis keamanan Data dan informasi dengan prinsip keamanan minimal terdiri atas terpenuhinya aspek kerahasiaan, keaslian, keutuhan, kenirsangkalan, dan ketersediaan.

1. Kerahasiaan

Terpenuhinya aspek kerahasiaan sebagaimana dimaksud dilakukan dengan prosedur:

- a. menetapkan klasifikasi informasi;
- b. menerapkan enkripsi dengan sistem kriptografi; dan
- c. menerapkan pembatasan akses terhadap Data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan.

2. Keaslian

Terpenuhinya aspek keaslian sebagaimana dimaksud dilakukan dengan prosedur:

- a. menyediakan mekanisme verifikasi;
- b. menyediakan mekanisme validasi; dan
- c. menerapkan sistem *hash function*.

3. Keutuhan

Terpenuhinya aspek keutuhan sebagaimana dimaksud dilakukan dengan prosedur:

- a. menerapkan pendeteksian modifikasi; dan
- b. menerapkan tanda tangan elektronik tersertifikasi.

4. Kenirsangkalan

Terpenuhinya aspek kenirsangkalan sebagaimana dimaksud dilakukan dengan prosedur:

- a. menerapkan tanda tangan elektronik tersertifikasi; dan
- b. penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.

5. Ketersediaan

Terpenuhinya aspek ketersediaan sebagaimana dimaksud dilakukan dengan prosedur:

- a. menerapkan sistem pencadangan secara berkala;
- b. membuat perencanaan untuk menjamin Data dan informasi dapat selalu diakses; dan
- c. menerapkan sistem pemulihan.

Keamanan merupakan elemen penting dalam proses berbagipakai Data yang bertujuan untuk melindungi integritas, kerahasiaan, dan

ketersediaan Data sepanjang siklus hidupnya. Dalam konteks berbagipakai Data, pengamanan teknis dan operasional harus diterapkan untuk melindungi Data dari ancaman kebocoran, akses tidak sah, atau penyalahgunaan selama proses transfer antar sistem, organisasi, atau wilayah hukum.

1. Pengamanan Teknis

Pengamanan teknis melibatkan penerapan teknologi yang dirancang untuk melindungi Data selama proses transfer, meliputi:

- a. Enkripsi Data: Data harus dienkripsi menggunakan algoritma yang kuat selama proses transfer, baik dalam transit (misalnya melalui protokol HTTPS atau VPN) maupun saat disimpan. Enkripsi ini memastikan bahwa Data hanya dapat diakses oleh pihak yang memiliki kunci enkripsi yang sesuai.
- b. Autentikasi dan/atau Otorisasi: Sistem harus memastikan bahwa hanya pihak yang berwenang yang dapat mengakses Data. Hal ini dapat dilakukan melalui mekanisme autentikasi multifaktor (MFA), sertifikat digital, atau kontrol akses berbasis peran (*role-based access control*).
- c. Monitoring Keamanan Jaringan: Penggunaan firewall, sistem deteksi intrusi (IDS), dan sistem pencegahan intrusi (IPS) untuk memantau aktivitas jaringan selama transfer Data dan mendeteksi aktivitas mencurigakan.
- d. Pengelolaan Kunci Kriptografi: Protokol untuk pengelolaan kunci kriptografi yang aman, termasuk pembaruan dan rotasi kunci secara berkala untuk mencegah risiko kompromi.

2. Pengamanan Operasional

Pengamanan operasional mencakup langkah-langkah tata kelola dan prosedur untuk mendukung keamanan selama berbagipakai Data, antara lain:

- a. Prosedur Verifikasi Identitas: Pihak yang mengakses atau menerima Data harus diverifikasi identitasnya sebelum transfer dilakukan.
- b. Penjaminan Mutu: Memastikan Data yang dikirimkan sesuai dengan persetujuan yang tertuang dalam berita acara serah terima.
- c. Protokol Transfer: Penggunaan protokol transfer dilaksanakan dengan mempertimbangkan aspek keamanan data dan informasi sesuai dengan peraturan perundang-undangan yang berlaku.
- d. Dokumentasi dan Audit: Setiap aktivitas berbagipakai Data harus terdokumentasi dengan baik, termasuk log akses, pihak-pihak yang terlibat, waktu transfer, dan detail teknis lainnya. Hal ini memungkinkan audit yang transparan dan identifikasi cepat jika terjadi pelanggaran keamanan.
- e. Manajemen Risiko dan Kontingensi: Rencana respon insiden harus disiapkan untuk menangani potensi pelanggaran keamanan selama proses transfer, termasuk langkah mitigasi.

3. Uji Keamanan dan Pelatihan

- a. Pengujian Penetrasi (*Penetration Testing*): Sistem yang digunakan untuk transfer Data harus diuji secara berkala untuk mengidentifikasi kerentanan dan memastikan keamanannya terhadap ancaman siber.
- b. Pelatihan Keamanan: Seluruh personel yang terlibat dalam proses transfer Data harus mengikuti pelatihan keamanan

yang mencakup identifikasi ancaman, praktik keamanan siber, dan kepatuhan terhadap regulasi yang berlaku.

4. Kepatuhan terhadap Standar dan Regulasi

Pengelola Data harus memastikan bahwa langkah-langkah pengamanan sesuai dengan standar nasional Indonesia, standar keamanan informasi internasional, serta mematuhi peraturan perundangan seperti UU PDP dan Undang-Undang Nomor 1 Tahun tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

B. Transparansi

Transparansi merupakan prinsip fundamental dalam berbig data yang bertujuan untuk membangun kepercayaan antara Pengelola Data dan/atau Prosesor DTSEN, Pengguna DTSEN, Subjek Data Pribadi, dan pihak-pihak terkait lainnya. Dengan menerapkan transparansi, pengelola Data dapat memastikan bahwa hak privasi individu dihormati dan meminimalkan potensi penyalahgunaan Data.

1. Penggunaan DTSEN

Instansi Pusat dan Pemerintah Daerah dalam memohon DTSEN harus diberi penjelasan yang jelas mengenai bagaimana DTSEN akan dimanfaatkan. Informasi ini mencakup jenis Data yang diminta untuk intervensi, proses pengolahan yang akan dilakukan, dan hasil akhir yang diharapkan. Misalnya, penggunaan untuk keperluan statistik akan diolah secara agregat dan anonim, sehingga identitas individu tidak dapat diidentifikasi. Penjelasan ini harus diberikan sebelum Data diserahkan, baik melalui konsultasi, atau media komunikasi lainnya.

2. Tujuan Pengolahan DTSEN

Tujuan pengumpulan dan pemrosesan Data harus dijelaskan secara spesifik. Hal ini mencakup informasi mengenai:

- a. Apakah DTSEN digunakan untuk keperluan layanan publik, penelitian, analisis kebijakan, atau tujuan lainnya.
- b. Apakah DTSEN akan digunakan untuk keperluan komersial atau pengembangan teknologi.
- c. Rencana penggunaan DTSEN dalam jangka pendek maupun jangka panjang.

Penjelasan mengenai tujuan ini harus mematuhi prinsip minimalisasi Data, di mana hanya Data yang relevan dan diperlukan untuk tujuan tertentu yang boleh dikumpulkan dan diolah.

3. Pihak yang Akan Menerima DTSEN

Calon Pengguna DTSEN juga perlu diberi informasi tentang struktur Data yang akan diterima. Hal ini mencakup penjelasan bagaimana struktur Data, pengelolaan Data oleh pihak Pengguna DTSEN, termasuk langkah-langkah pengamanan yang akan diterapkan untuk melindungi Data dari penyalahgunaan atau akses yang tidak sah. Layanan pemanfaatan DTSEN melalui Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengelola DTSEN. Pengguna DTSEN hanya dapat memberikan transfer Data kepada unit kerja/perangkat yang bertugas sebagai Produsen Data dalam satu instansi Pengguna DTSEN.

C. Kepatuhan Hukum

Kepatuhan hukum merupakan prinsip yang mendasari seluruh aktivitas berbig data untuk memastikan bahwa prosesnya berjalan sesuai dengan peraturan yang berlaku. Dalam konteks berbig data,

berdasarkan Pasal 20 UU PDP, kepatuhan hukum mencakup pemenuhan persyaratan dasar hukum, seperti persetujuan dari Subjek Data Pribadi (*user consent*), pemenuhan atau kewajiban yang diatur oleh undang-undang, pemenuhan hak dan kewajiban Pengendali dan/atau Prosesor DTSEN.

1. Tanggung Jawab Pengendali DTSEN

Pengendali DTSEN bertanggung jawab penuh atas pengelolaan DTSEN yang dimilikinya, mulai dari pengumpulan, pemrosesan, hingga penyimpanan dan penghapusan Data. Pengendali Data wajib memiliki dasar pemrosesan (Pasal 20 UU PDP) dan harus memastikan bahwa seluruh tahapan ini dilakukan dengan standar keamanan yang tinggi dan sesuai dengan peraturan perundang-undangan.

2. Prinsip Keamanan dalam Pemrosesan DTSEN

Dalam memproses DTSEN, Pengendali Data wajib menerapkan langkah-langkah keamanan yang memadai untuk mencegah akses tidak sah, kebocoran, pengubahan, hingga penghapusan Data oleh pihak yang tidak berwenang. Ini mencakup penerapan teknologi enkripsi, autentikasi, serta pengawasan terhadap sistem keamanan informasi.

3. Pencegahan dan Mitigasi Risiko Pelanggaran Data

Pengendali Data harus memiliki mekanisme pencegahan dan mitigasi risiko, termasuk adanya kebijakan dan prosedur yang memastikan deteksi dini, respons cepat, dan pemulihan Data jika terjadi insiden kebocoran atau penyalahgunaan DTSEN.

4. Kewajiban Memberitahukan Pelanggaran Data ke Pejabat atau Petugas Pelindung DTSEN

Jika terjadi pelanggaran perlindungan DTSEN, Pengendali Data wajib memberitahu Pejabat atau Petugas Pelindung DTSEN/otoritas terkait dalam waktu paling lambat 3x24 jam di hari kerja sejak mengetahui insiden tersebut. Pemberitahuan ini harus mencakup dampak pelanggaran, langkah mitigasi yang diambil.

BAB II PENYELENGGARA BERBAGIPAKAI DATA TUNGGAL SOSIAL DAN EKONOMI NASIONAL

Penyelenggara Berbagipakai DTSEN terdiri dari Pengendali DTSEN, Prosesor DTSEN, dan Pengguna DTSEN. Ketiganya bertanggung jawab memastikan hak Subjek Data Pribadi terpenuhi sebagaimana peraturan perundang-undangan yang berlaku. Kompetensi yang diperlukan penyelenggara berbagipakai DTSEN meliputi kemampuan teknis, hukum dan tata kelola perlindungan Data, serta memahami prinsip pemrosesan DTSEN.

A. Pengendali DTSEN

Pengendali DTSEN adalah setiap orang, badan publik yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan DTSEN. Penunjukan Pengendali DTSEN dilakukan secara resmi melalui instruksi Presiden, Peraturan Menteri ataupun Kesepakatan Kementerian/Lembaga.

1. Kriteria

Pengendali DTSEN adalah pihak yang bertanggung jawab atas pengendalian dan pengelolaan DTSEN. Berdasarkan Pasal 1 Angka 4 UU PDP yang dapat menjadi Pengendali DTSEN adalah Badan Publik diantaranya lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, atau organisasi nonpemerintah sepanjang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, sumbangan masyarakat, dan/atau luar negeri.

2. Kewajiban

a. Menjamin Hak Subjek Data Pribadi

Pengendali wajib memastikan bahwa Subjek Data Pribadi memiliki hak sesuai dengan peraturan perundang-undangan di bidang perlindungan Data pribadi untuk:

- 1) Mengakses Data.
- 2) Menarik persetujuan (*withdraw consent*).
- 3) Memperbaiki atau menghapus Data.

b. Memastikan Keamanan DTSEN

- 1) Pengendali harus melakukan tindakan pencegahan terhadap akses yang tidak sah.
- 2) Pengendali harus Melindungi Data dari kebocoran, manipulasi, atau kehilangan.
- 3) Menjamin kerahasiaan Data.

c. Transparansi dalam Pengolahan Data

- 1) Memberikan informasi yang jelas kepada Subjek Data Pribadi mengenai tujuan dan dasar hukum pengolahan Data.
- 2) Mendokumentasikan aktivitas pengolahan Data secara tertib.

d. Penunjukan Pejabat Petugas Pelindung Data (PPDP)

Jika diwajibkan, pengendali Data harus menunjuk PPDP untuk memastikan kepatuhan terhadap UU PDP.

e. Penyampaian Pemberitahuan dalam Kasus Pelanggaran Data

Pengendali wajib memberitahukan pelanggaran DTSEN kepada Subjek Data Pribadi dan otoritas terkait paling lambat 3x24 jam

setelah mengetahui adanya pelanggaran sesuai peraturan perundang-undangan yang berlaku.

3. Pihak

Pengendali DTSEN merupakan kementerian yang menyelenggarakan urusan pemerintahan di bidang perencanaan pembangunan nasional, kementerian yang menyelenggarakan sinkronisasi dan koordinasi serta pengendalian urusan kementerian dalam penyelenggaraan pemerintahan di bidang pemberdayaan masyarakat, kementerian yang menyelenggarakan urusan pemerintahan di bidang sosial, dan badan yang menyelenggarakan tugas pemerintahan di bidang statistik yang ditetapkan dengan keputusan menteri.

B. Prosesor DTSEN

Kriteria, kewajiban, dan pihak Prosesor DTSEN merupakan satu kesatuan yang tidak terpisahkan dengan ketentuan kriteria, kewajiban, dan pihak sebagai Pengendali DTSEN yang diatur dalam Bab 2 huruf A tentang Pengendali DTSEN.

C. Pengguna DTSEN

Pengguna DTSEN adalah setiap orang, badan publik, atau organisasi internasional yang melakukan pemrosesan DTSEN atas nama Pengendali DTSEN. Berikut penjabaran kriteria, kewajiban, dan pihak yang terlibat pada Pengguna DTSEN.

1. Kriteria

- a. Pengguna DTSEN memanfaatkan DTSEN berdasarkan tugas dan kewenangannya sesuai dengan ketentuan peraturan perundang-undangan.
- b. Pengguna DTSEN terikat oleh prinsip dan kewajiban yang berlaku untuk Pengendali DTSEN, seperti: Akurasi, keamanan, dan kerahasiaan Data, serta Pemenuhan hak Subjek Data Pribadi.
- c. Pengguna DTSEN menjadi Pengendali DTSEN atas DTSEN yang diterimanya.

2. Kewajiban

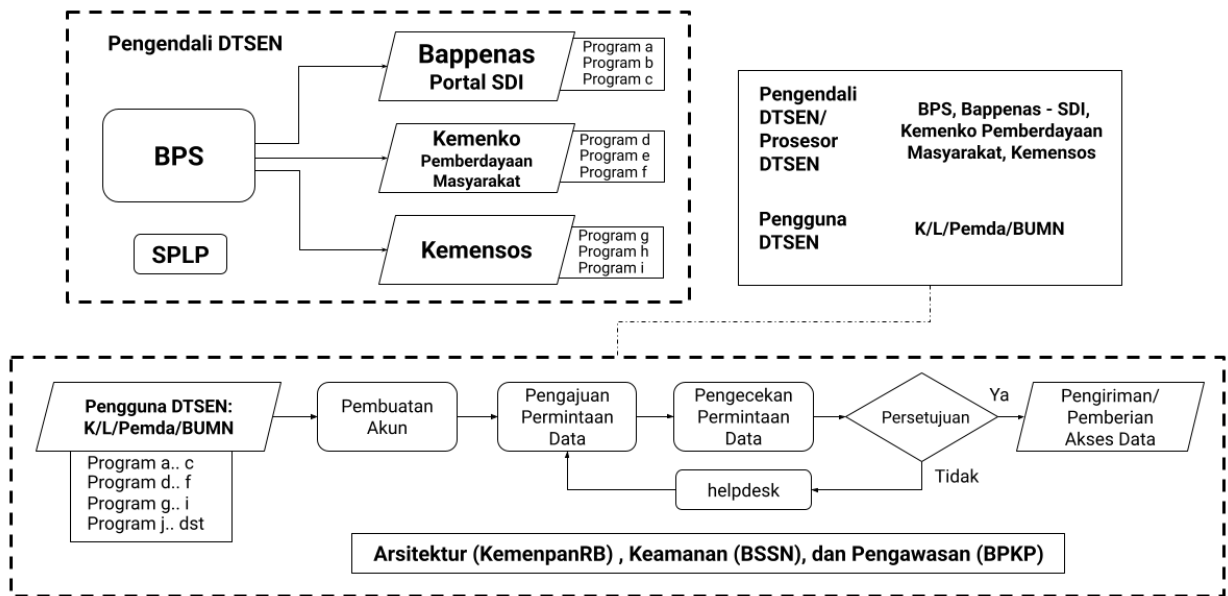
Pengguna DTSEN wajib melakukan perlindungan Data pribadi sesuai dengan ketentuan peraturan perundang-undangan yang mengatur mengenai perlindungan Data pribadi.

3. Pihak

Pengguna DTSEN merupakan Walidata Instansi Pusat, Walidata Pemerintah Daerah, koordinator forum Pemerintah Daerah, unit kerja yang ditunjuk oleh Menteri/Kepala dan/atau Perangkat Daerah ditunjuk oleh Kepala Daerah dan/atau unit kerja yang menyelenggarakan tugas dan fungsi di bidang pengelolaan Data dan informasi di badan usaha milik negara.

BAB III
PENYELENGGARAAN BERBAGIPAKAI
DATA TUNGGAL SOSIAL DAN EKONOMI NASIONAL

A. Konsep Alur Penyelenggaraan Berbagipakai DTSEN



Gambar 3.1. Aliran DTSEN

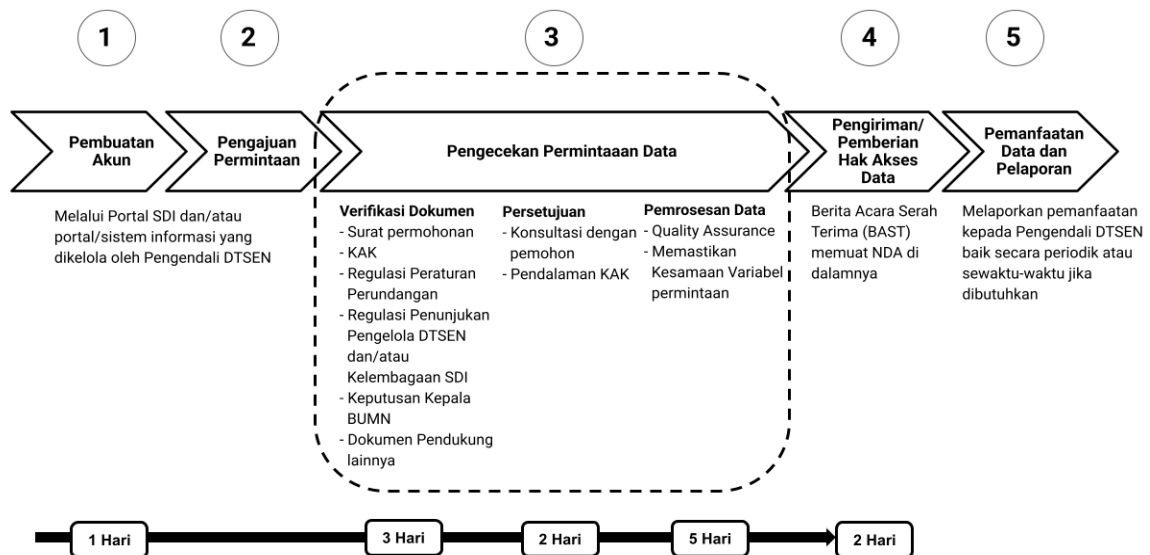
Data sebagaimana Instruksi Presiden Nomor 4 Tahun 2025 tentang DTSEN dikumpulkan dari Kementerian dan Lembaga dipadankan oleh Badan Pusat Statistik (BPS). Data dikelola oleh Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN melalui ekosistem Pusat Data Nasional (PDN) menggunakan jaringan Sistem Penghubung Layanan Pemerintah (SPLP).

Akses terhadap DTSEN dilakukan melalui Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN, yang berfungsi sebagai gerbang utama bagi Pengguna DTSEN untuk mengajukan permintaan Data. Sebelum pengajuan permintaan Data diperlukan pelaksanaan reviu kesiapan dan kelayakan infrastruktur dan keamanan. Apabila telah layak maka setiap Pengguna DTSEN yang membutuhkan DTSEN harus menyampaikan pengajuan permintaan Data dengan rincian tujuan penggunaan serta program yang diusung untuk memanfaatkan DTSEN. Pengajuan ini kemudian masuk dalam tahap pengecekan administrasi dan validasi untuk memastikan kesesuaian dengan kebijakan berbagipakai Data serta peraturan perundang-undangan yang berlaku.

Setelah itu, dilakukan tahap pengecekan. Jika terdapat kekurangan dalam pengajuan permintaan Data, Pengguna DTSEN akan mendapatkan pemberitahuan untuk perbaikan atau pelengkapan dokumen. Jika dinyatakan memenuhi persyaratan, maka Data akan diproses lebih lanjut dalam tahap pemrosesan. Tahapan ini mencakup pemilahan Data, agregasi Data, penyesuaian format Data, pemastian keamanan akses, serta penyediaan Data yang sesuai dengan kebutuhan Pengguna DTSEN.

Tahap akhir dalam alur berbagipakai DTSEN adalah pemberian akses Data. Data yang telah diproses akan disediakan untuk Pengguna DTSEN sesuai dengan hak akses yang diberikan. DTSEN dapat diakses melalui mekanisme yang telah ditentukan dalam sistem Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN. DTSEN tersebut dilengkapi dengan informasi yang berkaitan dengan versi rilis,

standar Data, dan metadata. Dengan alur ini, proses berbagi Data menjadi lebih sistematis, aman, dan terstruktur, memastikan bahwa DTSEN dapat digunakan secara optimal untuk mendukung berbagai program pemerintah yang memerlukan Data sosial ekonomi nasional yang akurat dan mutakhir.



Gambar 3.2. Tahapan Pemrosesan DTSEN

1. Pembuatan Akun

Proses pembuatan akun Layanan DTSEN memerlukan waktu pelayanan yang ditargetkan selama 1 hari kerja. Pembuatan akun dilakukan oleh Pengguna DTSEN dalam hal ini Walidata Instansi Pusat, Walidata Pemerintah Daerah, koordinator forum Pemerintah Daerah, unit kerja yang ditunjuk oleh Menteri/Kepala dan/atau Perangkat Daerah ditunjuk oleh Kepala Daerah, dan/atau dan/atau unit kerja yang menyelenggarakan tugas dan fungsi di bidang pengelolaan Data dan informasi di badan usaha milik negara. Pengguna DTSEN dari badan usaha milik negara secara khusus yang diberikan tugas oleh pemerintah terkait program bantuan sosial, bantuan pemerintah, dan subsidi.

Kelengkapan dokumen yang diperlukan adalah surat permohonan pembuatan akun layanan pemanfaatan DTSEN yang ditandatangani oleh Sekretaris Jenderal/Sekretaris Utama Kementerian/Sekretaris Lembaga/Sekretaris Daerah/Direktur Utama BUMN disertai nama, email (dengan nama pengguna berdomain .go.id), jabatan, unit kerja, nomor HP, dan NIP atau NIK untuk BUMN. Untuk keperluan koordinasi teknis dan verifikasi kepada pihak pengelola Layanan DTSEN diperlukan narahubung dengan menyertakan nama, nomor HP, dan email (berdomain go.id).

Akun yang tidak digunakan selama 30 hari akan menjadi nonaktif. Sebelum akun menjadi nonaktif, sistem Layanan DTSEN akan memberikan notifikasi otomatis kepada pemegang akun agar segera mengakses akun.

Terkait format surat permohonan pembuatan dan perubahan akun layanan pemanfaatan DTSEN disusun dengan mengikuti format sebagaimana terlampir dalam tautan berikut <https://link.bappenas.go.id/ReferensiBagipakaiDTSEN>.

2. Pengajuan Permintaan Data

Pengguna DTSEN mengajukan permintaan Data melalui Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN. Surat pengajuan permintaan data disusun dengan

mengikuti format sebagaimana terlampir dalam tautan berikut <https://link.bappenas.go.id/ReferensiBagipakaiDTSEN>.

Pengguna DTSEN dalam hal ini Walidata Instansi Pusat, Walidata Pemerintah Daerah, koordinator forum Pemerintah Daerah, dan unit kerja yang ditunjuk oleh Menteri/Kepala dan/atau Perangkat Daerah ditunjuk oleh Kepala Daerah, mengajukan permintaan DTSEN kriteria data mikro dan data dengan nama dan alamat (*by name by address*) melampirkan dokumen:

- a. Surat permohonan Data yang ditandatangani menteri/kepala lembaga/kepala daerah;
- b. Kerangka acuan kerja;
- c. Peraturan perundang-undangan sebagai dasar pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengguna DTSEN;
- d. Penetapan pembentukan kelembagaan tentang pelaksana pengelolaan pemanfaatan DTSEN di tingkat kementerian/lembaga/pemerintah daerah;
- e. Peraturan menteri/kepala lembaga/kepala badan/kepala daerah tentang SDI; dan
- f. Dokumen pendukung lainnya.

Pengguna DTSEN dalam hal ini Walidata Pemerintah Daerah dan/atau perangkat daerah yang ditunjuk dalam mengajukan permintaan DTSEN harus berkoordinasi dengan koordinator forum SDI tingkat Daerah.

Pengguna DTSEN dalam hal ini badan usaha milik negara yang dilakukan oleh unit kerja yang menyelenggarakan tugas dan fungsi di bidang pengelolaan Data dan informasi, mengajukan permintaan DTSEN kriteria data mikro dan data dengan nama dan alamat (*by name by address*) melampirkan dokumen:

- a. Surat permohonan Data yang ditandatangani kepala badan usaha milik negara;
- b. Kerangka acuan kerja;
- c. Peraturan perundang-undangan sebagai dasar pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengguna DTSEN;
- d. Penetapan pembentukan kelembagaan tentang pelaksana pengelolaan pemanfaatan DTSEN;
- e. Keputusan kepala badan usaha milik negara yang menunjuk unit kerja yang menyelenggarakan tugas dan fungsi di bidang pengelolaan Data dan informasi yang diberikan tugas oleh pemerintah terkait program bantuan sosial, bantuan pemerintah, dan/atau subsidi; dan
- f. Dokumen pendukung lainnya.

Terkait dokumen pengajuan permintaan DTSEN kriteria data mikro dan data dengan nama dan alamat (*by name by address*) sebagaimana tersebut di atas disusun dengan mengikuti format sebagaimana terlampir dalam tautan berikut <https://link.bappenas.go.id/ReferensiBagipakaiDTSEN>.

3. Pengecekan Permintaan Data

Pengendali DTSEN melakukan verifikasi teknis dan substansi. Verifikasi teknis berkaitan dengan pengecekan kelengkapan administrasi terhadap dokumen yang diajukan Pengguna DTSEN. Verifikasi substansi berkaitan dengan pendalaman KAK dan

pengecekan Dasar hukum/dasar pemrosesan perlu bersesuaian dengan variabel DTSEN.

Pengguna DTSEN dalam pengajuan permintaan DTSEN terbatas pada variabel tertentu sesuai dengan catatan tim verifikasi substansi dan persetujuan Koordinator. Pemerintah Daerah sebagai Pengguna DTSEN secara khusus dalam pengajuan permintaan DTSEN mendapatkan seluruh variabel sesuai dengan wilayah administrasi Pengguna DTSEN.

a. Verifikasi Teknis

Pada tahapan ini Pengguna DTSEN dapat memperbaiki dan/atau melengkapi dokumen. Tim verifikasi teknis memberikan catatan untuk setiap dokumen kelengkapan. Jika terdapat dokumen yang keliru dan/atau atau tidak lengkap, maka tim verifikasi teknis dapat berkonsultasi dengan tim verifikasi substansi dalam berkomunikasi dengan Pengguna DTSEN untuk mengunggah kembali dokumen yang tepat. Jika dokumen dinyatakan tepat dan lengkap, proses dapat dilanjutkan ke tahap berikutnya.

b. Verifikasi Substansi

Pada tahapan ini target waktu pelayanan mulai diterapkan. Tim verifikasi substansi menerima catatan tim verifikasi teknis untuk setiap dokumen pengajuan permohonan. Pada tahapan ini Pengguna DTSEN tidak dapat memperbaiki ataupun melengkapi dokumen. Sehingga apabila dokumen ditolak oleh tim verifikasi substansi, jika diperlukan tim verifikasi substansi dapat mengundang Pengguna DTSEN untuk melakukan klarifikasi dokumen. Hasil klarifikasi tersebut dituangkan ke dalam berita acara.

c. Persetujuan Koordinator

Koordinator sebagaimana dimaksud merupakan pejabat tinggi madya/pratama yang ditunjuk oleh Menteri PPN/Kepala Bappenas. Koordinator menerima catatan tim verifikasi substansi dan/atau berita acara klarifikasi dokumen. Koordinator mencermati dan menentukan persetujuan dokumen pemohon. Jika dokumen pemohon diterima oleh Koordinator maka secara bersamaan Data akan mulai diproses pemilahan dan agregasi. Jika dokumen pemohon ditolak oleh koordinator maka proses permintaan DTSEN dianggap selesai dan tidak dapat dilanjutkan kembali.

d. Pemrosesan Data

Pada tahapan ini data dipilah dan diagregasi sesuai dengan dokumen pengajuan permohonan DTSEN. Tim penjaminan mutu/*Quality Assurance* (QA) memastikan Data yang dihasilkan bersesuaian dengan variabel dokumen pengajuan permohonan DTSEN.

4. Pengiriman Data

Pada tahapan ini Pengguna DTSEN dapat menerima Data/Hak Akses Data setelah dokumen berita acara serah terima telah ditandatangani oleh Koordinator DTSEN dan Pengguna DTSEN serta Data telah lolos penjaminan mutu. DTSEN dapat diakses melalui mekanisme yang telah ditentukan dalam sistem Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN. Mekanisme yang digunakan yaitu integrasi antar sistem

(*Application Programming Interface Service*) dengan memanfaatkan sistem penghubung layanan pemerintah.

Tautan akses Data diberikan masa aktif selama 30 hari. Jika diperlukan Pengguna DTSEN dapat menambah masa aktif tautan dengan berkomunikasi kepada narahubung layanan DTSEN.

5. Pemanfaatan Data dan Pelaporan

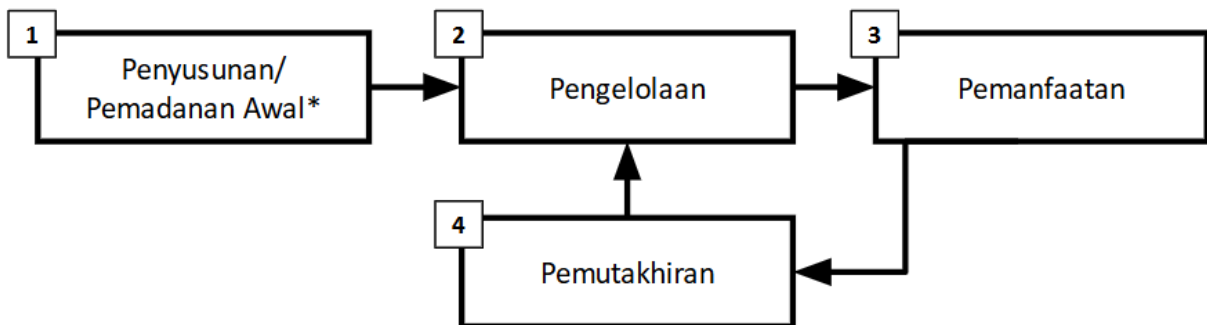
Pengguna DTSEN dalam memanfaatkan DTSEN melaporkan pemanfaatan Data kepada Pengendali DTSEN dan wajib menjaga keamanan Data sesuai dengan kaidah perundang-undangan.

Data yang digunakan adalah DTSEN rilis terakhir. Data versi lama sebelum rilis terakhir dianggap tidak berlaku dan wajib dilakukan pemusnahan sesuai dengan ketentuan UU PDP.

B. Konsep Arsitektur Layanan Pemanfaatan DTSEN Berbasis Arsitektur Sistem Pemerintahan Berbasis Elektronik

Konsep arsitektur layanan pemanfaatan DTSEN mengikuti arsitektur Sistem Pemerintahan Berbasis Elektronik (SPBE) terdiri dari penyusunan/pemadanan awal, pengelolaan, dan pemanfaatan. Tata kelola Data Tunggal Sosial dan Ekonomi Nasional merupakan sebuah sistem yang dirancang untuk memastikan pengelolaan Data sektoral dan nasional yang efisien, akurat, dan relevan guna mendukung perencanaan pembangunan yang berbasis Data.

1. Keterhubungan Sistem

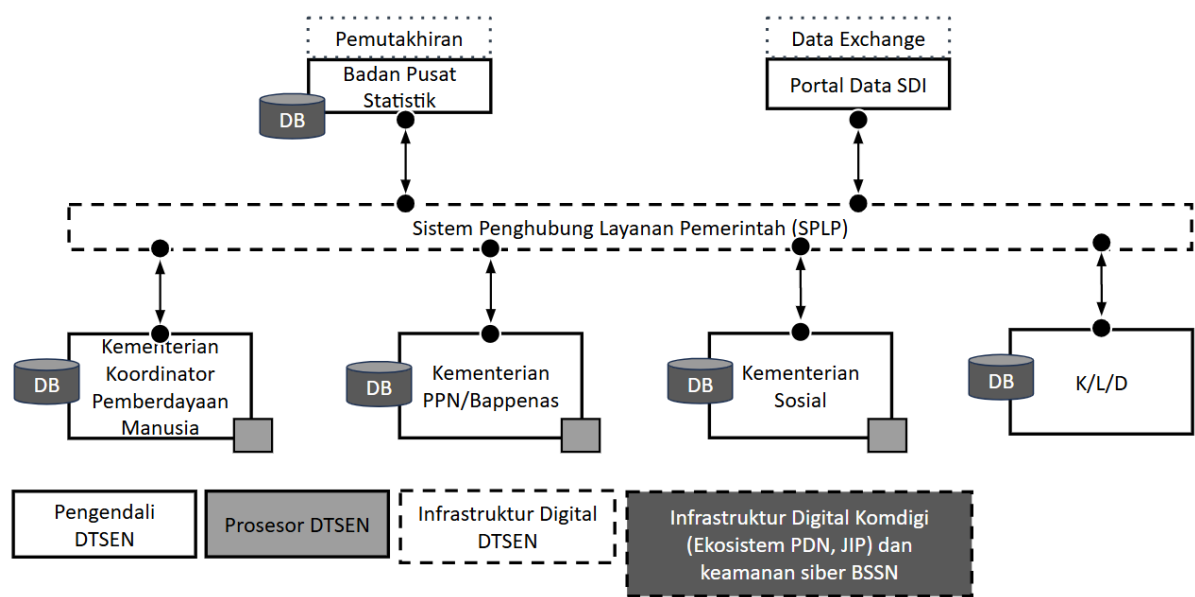


Gambar 3.3. Arsitektur Layanan Pemanfaatan DTSEN

Arsitektur layanan pemanfaatan DTSEN berbasis SPBE dalam ekosistem SPBE dirancang untuk memastikan pengelolaan Data yang terintegrasi dan sistematis. Proses ini dimulai dengan tahap penyusunan atau pemadanan awal Data untuk menjamin keselarasan dan kelengkapan sebelum dikelola lebih lanjut. Data yang telah melalui tahap awal ini kemudian masuk ke dalam tahap pengelolaan, yang mencakup pengolahan, penyimpanan, serta penerapan standar tata kelola guna memastikan interoperabilitas dan kualitas Data yang optimal.

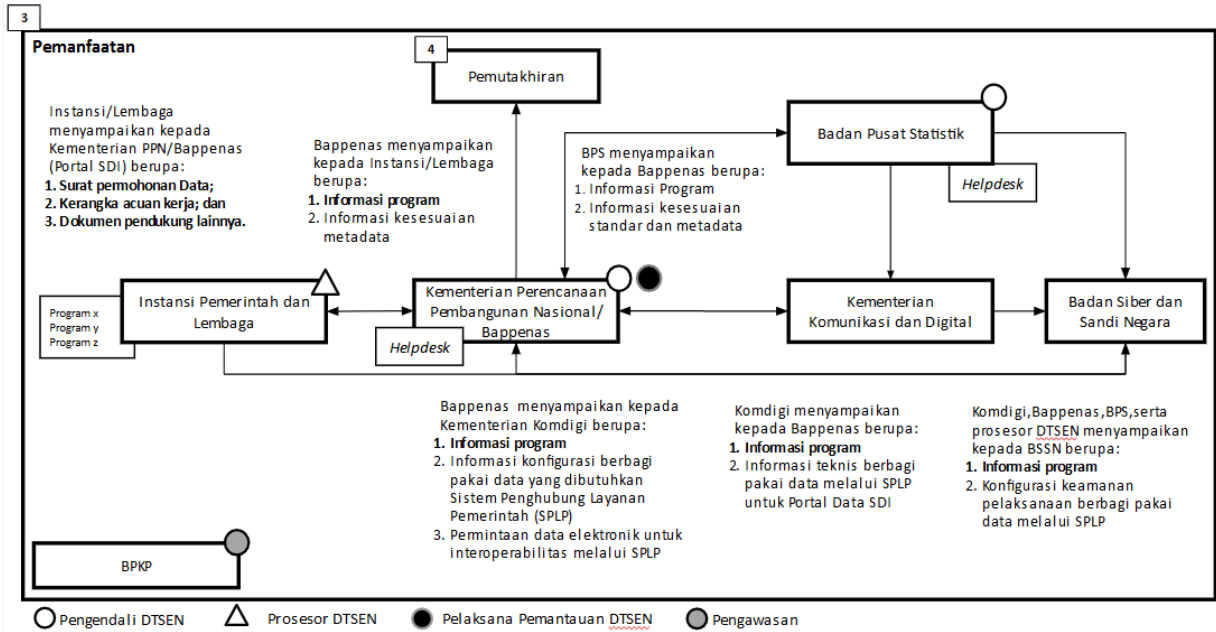
Setelah dikelola, Data akan digunakan dalam dua proses utama, yaitu pemanfaatan dan pemutakhiran. Pemanfaatan Data memungkinkan berbagai instansi pemerintah dan pemangku kepentingan menggunakannya untuk penyusunan kebijakan berbasis Data serta perencanaan pembangunan yang lebih efektif. Sementara itu, pemutakhiran dilakukan secara berkala untuk menjaga validitas, akurasi, dan relevansi Data sesuai dengan perkembangan terkini. Dengan pendekatan ini, DTSEN membentuk siklus berkelanjutan dalam pengelolaan Data yang akuntabel, transparan, dan sesuai dengan kebijakan transformasi digital pemerintah.

Untuk mendukung implementasi sistem ini, SPLP digunakan sebagai infrastruktur utama yang menghubungkan antar sistem. BPS sebagai penyedia Data hasil pemutakhiran dan Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN sebagai sarana bagipakai Data. Kementerian Koordinator Pemberdayaan Manusia, Kementerian Perencanaan Pembangunan Nasional/Badan Perencanaan Pembangunan Nasional (Kementerian PPN/Bappenas), Kementerian Sosial, serta instansi pemerintah lainnya, dapat mengakses dan memanfaatkan Data ini sesuai dengan kebutuhan kebijakan dan perencanaan pembangunan. Infrastruktur digital, seperti ekosistem PDN, Jaringan Intra Pemerintah (JIP), serta sistem keamanan siber, turut berperan dalam menjamin kelancaran dan keamanan pertukaran Data, mendukung efisiensi pemerintahan digital, serta meningkatkan efektivitas tata kelola Data nasional.



Gambar 3.4. Arsitektur Teknologi Pertukaran Data DTSEN Berbasis kerangka Arsitektur SPBE

2. Pemanfaatan



Gambar 3.5. Arsitektur Pemanfaatan DTSEN

Pemanfaatan Data yang sudah dimutakhirkan oleh BPS, dikelola oleh Kementerian Perencanaan Pembangunan Nasional/Badan Perencanaan Pembangunan Nasional, Kementerian Koordinator Bidang Pemberdayaan Masyarakat, dan Kementerian Sosial untuk dapat dibagikan kepada Instansi Pusat, Pemerintah Daerah, dan Badan Usaha Milik Negara yang selanjutnya dapat dimanfaatkan untuk kepentingan perencanaan, pemantauan, evaluasi, dan pengendalian pembangunan. Pemanfaatan dilakukan melalui Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN.

BAB IV
KLASIFIKASI DATA DAN MANAJEMEN HAK AKSES

A. Klasifikasi Data

Pengguna DTSEN dalam mengajukan permintaan DTSEN kepada Pengendali DTSEN mendapatkan hak akses sesuai dengan kebutuhan intervensi program yang tertuang dalam KAK dan peraturan perundang-undangan sebagai dasar pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengguna DTSEN. Dalam mengajukan permintaan hak akses DTSEN, Pengguna DTSEN harus memastikan telah memenuhi persyaratan yang ditetapkan sebagaimana dijabarkan dalam regulasi yang berlaku.

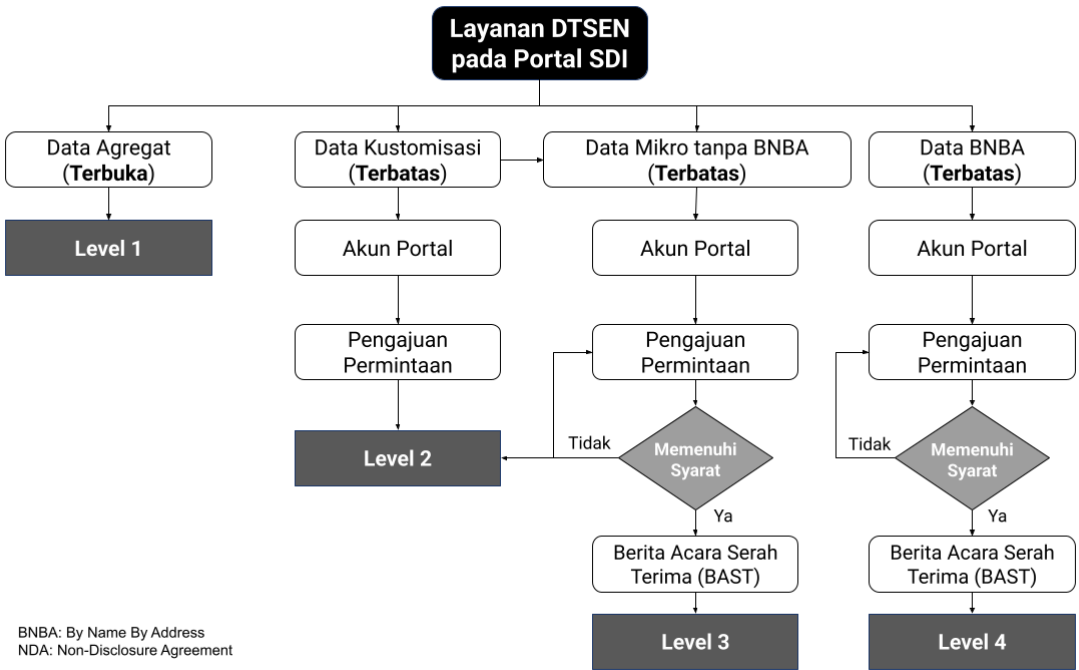
Tabel 4.1 Level Hak Akses DTSEN

Ketentuan	Level Hak Akses DTSEN			
	Level 1 Agregat (Terbuka)	Level 2 Kustomisasi (Terbatas)	Level 3 Data Mikro Tanpa Nama dan Alamat (Terbatas)	Level 4 Berdasarkan Nama dan Alamat (Terbatas)
Media Akses	Portal dengan akses publik terbuka.	1. Portal dan/atau sistem informasi dengan hak akses khusus. Membutuhkan akun dan aktivitas login; atau 2. Fasilitas pemilahan dan agregasi DTSEN	1. Portal dan/atau sistem informasi dengan hak akses khusus. Membutuhkan akun dan aktivitas login; atau 2. Fasilitas pemilahan dan agregasi DTSEN	1. Portal dan/atau sistem informasi dengan hak akses khusus. Membutuhkan akun dan aktivitas login; atau 2. Fasilitas pemilahan dan agregasi DTSEN
Mekanisme	Tidak perlu pengajuan hak akses.	Perlu pengajuan permintaan hak akses	Perlu pengajuan permintaan hak akses	Perlu pengajuan permintaan hak akses
Persyaratan	Tanpa persyaratan	Kapasitas: Mampu melakukan pemanfaatan Data Administrasi: 1. Surat pengajuan permintaan Data	Kapasitas: Mampu melakukan pemanfaatan Data Administrasi: 1. Surat pengajuan permintaan Data 2. KAK	Kapasitas: Mampu melakukan pemanfaatan Data Administrasi: 1. Surat pengajuan permintaan Data 2. KAK

Ketentuan	Level Hak Akses DTSEN			
	Level 1 Agregat (Terbuka)	Level 2 Kustomisasi (Terbatas)	Level 3 Data Mikro Tanpa Nama dan Alamat (Terbatas)	Level 4 Berdasarkan Nama dan Alamat (Terbatas)
			3. SK Penetapan Pelaksana Pengelolaan Pemanfaata n DTSEN 4. Peraturan tentang SDI 5. Dokumen Pendukung lainnya 6. BAST	3. SK Penetapan Pelaksana Pengelolaan Pemanfaata n DTSEN 4. Peraturan tentang SDI 5. Dokumen Pendukung lainnya 6. BAST

Hak akses DTSEN yang diajukan dapat mencakup lebih dari satu tingkatan. Jika Pengguna DTSEN mengajukan permintaan terhadap lebih dari satu tingkatan, maka pemohon wajib mengikuti dan memenuhi ketentuan serta persyaratan yang berlaku pada tingkatan hak akses tertinggi yang dimohonkan. Hal ini bertujuan untuk memastikan keamanan, kepatuhan regulasi, serta perlindungan DTSEN dalam setiap proses berbagipakai Data.

Hak akses DTSEN dapat diberikan melalui sistem yang diputuskan oleh Pemerintah, atau melalui fasilitas pengolahan DTSEN terpadu yang dikelola oleh Walidata. Mekanisme ini dirancang untuk memastikan bahwa akses dan pemanfaatan Data dilakukan secara terkontrol, transparan, dan sesuai dengan prinsip perlindungan DTSEN.



Gambar 4.1 Alur dan Prosedur Pengajuan Permintaan Hak Akses DTSEN

B. Manajemen Hak Akses

Manajemen hak akses Data pada layanan DSTEN akan diimplementasikan melalui pembagian peran (*role-based access control*). Setiap pengguna memiliki peran dan tanggung jawab yang berbeda sesuai dengan proses bisnis yang berlangsung. Pembagian peran tersebut akan diatur lebih lanjut dalam petunjuk pelaksanaan dan/atau petunjuk teknis.

BAB V
LAYANAN PEMANFAATAN
DATA TUNGGAL SOSIAL DAN EKONOMI NASIONAL

A. Prasyarat Sistem Informasi Berbagipakai DTSEN

Pelindungan Data pribadi menjadi prioritas utama dalam konteks berbagipakai, terutama dalam lingkungan ekosistem digital yang kompleks. Implementasi langkah-langkah keamanan seperti sertifikasi yang berstandar Internasional, fitur keamanan Data, sistem autentikasi yang kuat, audit trail, dan *approval system* dengan Tanda Tangan Elektronik (TTE) adalah kunci untuk memastikan integritas, kerahasiaan, dan akuntabilitas.

Selain itu, pemanfaatan JIP/VPN, SPLP yang merupakan amanat dari Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, dan pemantauan keamanan secara berkala melalui penilaian risiko atau *vulnerability assessment* memperkuat pelindungan terhadap potensi ancaman siber, sehingga mendukung kepatuhan terhadap regulasi dan menjaga kepercayaan Subjek Data Pribadi. Dalam hal keterbatasan infrastruktur untuk pemanfaatan JIP dan SPLP maka berbagipakai DTSEN pada masa transisi mengikuti ketentuan perundang-undangan yang berlaku.

Namun demikian, Pengendali DTSEN, Prosesor DTSEN, dan Pengguna DTSEN perlu memenuhi kewajiban Pelindungan Data Pribadi (PDP), seperti dasar pemrosesan, tujuan pemrosesan, dan penilaian dampak PDP sebagaimana diamanatkan pada ketentuan perundang-undangan.

1. Pelaksanaan Kegiatan Penerapan Keamanan

a. Edukasi Kesadaran Keamanan

Memastikan personil yang ditetapkan dalam pelaksanaan tugas pengelolaan pemanfaatan DTSEN memiliki kompetensi dan keahlian memadai terkait keamanan Data berdasarkan standar yang diatur oleh badan yang melaksanakan tugas pemerintahan di bidang keamanan siber dan persandian dan peraturan perundang-undangan yang mengatur mengenai pelindungan data pribadi.

b. Menerapkan *Secure SDLC* dan Standar Keamanan SPBE

Dalam pembangunan dan/atau pengembangan aplikasi atau sistem Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN harus menerapkan kerangka kerja *Secure Software Development Life Cycle (Secure SDLC)* untuk memastikan penerapan persyaratan keamanan atau mengintegrasikan praktik keamanan ke dalam setiap tahap pengembangan.

Persyaratan keamanan sebagai kontrol keamanan yang harus diterapkan pada sistem Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN, dan portal atau sistem informasi Pengguna DTSEN yang terhubung dengan Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN dilaksanakan dengan memperhatikan peraturan perundang-undangan yang ditetapkan oleh badan yang melaksanakan tugas pemerintahan di bidang keamanan siber dan persandian.

- c. Penerapan Modul Kriptografi
Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN serta sistem informasi Instansi Pusat dan Pemerintah Daerah yang terhubung dengannya harus menerapkan sistem modul kriptografi untuk mendukung enkripsi pada siklus Data *at rest*, *in transit* dan *in use*.
- d. Pengujian Teknis Keamanan
Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN dan portal atau sistem informasi Pengguna DTSEN yang terhubung dalam Penyelenggaraan DTSEN harus dilakukan pengujian teknis keamanan melalui *vulnerability assessment* sampai dengan *penetration testing* secara berkala untuk mengidentifikasi kerentanan dan potensi risiko keamanan terhadap sistem. Ruang lingkup pengujian melihat kepada identifikasi terhadap aset dan risiko dengan tingkat kritikalitas yang tinggi terkait dengan Penyelenggaraan DTSEN.
- e. Audit Keamanan
Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN dan portal atau sistem informasi Pengguna DTSEN yang terhubung dalam Penyelenggaraan DTSEN harus dilakukan audit internal keamanan aplikasi SPBE setiap 1 (satu) tahun sekali oleh Instansi Pemrakarsa Aplikasi, selanjutnya diajukan untuk dilakukan audit eksternal oleh Lembaga Audit TIK Pemerintah dan/atau Lembaga Audit TIK terakreditasi setiap 2 (dua) tahun sekali untuk memastikan kepatuhan dan kesesuaian terhadap regulasi dan standar keamanan.
- f. Penanganan Insiden
 - 1) Pra Insiden
 - a) Instansi Pemrakarsa dan Kementerian yang terlibat lainnya harus melakukan monitoring keamanan sistem Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN secara berkala menggunakan alat pemantauan keamanan yang sesuai.
 - b) Melakukan simulasi penanganan insiden secara berkala untuk memastikan kesiapan tim dalam menghadapi berbagai skenario insiden siber.
 - c) Menyusun dan memperbarui rencana tanggap insiden yang mencakup prosedur detail, peran dan tanggung jawab tim, serta jalur komunikasi yang jelas.
 - d) Mempersiapkan segala kebutuhan penanganan insiden, seperti mempersiapkan satu ruangan khusus untuk menangani insiden, serta mempersiapkan tools dan media yang dibutuhkan untuk menangani insiden.
 - 2) Saat Terjadi Insiden
 - a) Mengaktifkan tim tanggap insiden sesuai dengan rencana yang telah ditetapkan.
 - b) Melakukan identifikasi dan analisis insiden untuk menentukan jenis, sumber, dan dampak insiden.
 - c) Mengisolasi sistem yang terdampak untuk mencegah penyebaran insiden lebih lanjut.

- d) Melakukan mitigasi untuk mengurangi dampak insiden dan memulihkan layanan secepat mungkin.
 - e) Melakukan pelaporan insiden kepada pihak yang berwenang, baik internal maupun eksternal, sesuai dengan prosedur yang berlaku.
- 3) Pasca Insiden
- a) Mendokumentasikan seluruh proses penanganan insiden, termasuk detail insiden, langkah-langkah yang diambil, dan hasil yang dicapai.
 - b) Melakukan evaluasi menyeluruh terhadap penanganan insiden untuk mengidentifikasi kelemahan dan perbaikan yang diperlukan.
 - c) Memperbarui rencana tanggap insiden berdasarkan hasil evaluasi.
 - d) Melakukan pemulihan sistem secara menyeluruh, dan memastikan sistem kembali berjalan normal.
 - e) Memberikan laporan akhir penanganan insiden kepada pihak yang berkepentingan.

2. Fitur Tambahan Keamanan Database dan *Access Control*

Fitur keamanan dapat berkembang sesuai dengan perkembangan teknologi dan tidak terbatas pada fitur yang dapat disediakan saat ini.

- a. Enkripsi Data saat transit (misalnya, TLS/HTTPS) dan saat disimpan (AES-256)

Enkripsi Data saat transit menggunakan protokol TLS/HTTPS untuk melindungi DTSEN saat dikirimkan melalui jaringan. TLS (*Transport Layer Security*) mengenkripsi Data sehingga hanya pengirim dan penerima yang dapat membacanya, mencegah risiko penyadapan atau manipulasi Data. Implementasinya melibatkan konfigurasi sertifikat SSL/TLS pada server dan memastikan komunikasi melalui protokol HTTPS. Enkripsi Data saat disimpan menggunakan algoritma seperti AES-256 (*Advanced Encryption Standard*) yang menyediakan enkripsi tingkat tinggi dengan kunci 256-bit. Implementasinya dilakukan dengan mengenkripsi Data di server atau database menggunakan *software encryption tools* dan mengelola kunci enkripsi secara aman menggunakan *Key Management System* (KMS).

- b. Autentikasi dan otorisasi pengguna yang kuat.

Dilengkapi dengan *Two Factor Authentication* (2FA) atau *Multi Factor Authentication* (MFA) Autentikasi dan otorisasi pengguna yang kuat sangat penting dalam melindungi DTSEN karena memastikan hanya pengguna yang sah yang dapat mengakses sistem. Dengan *Two-Factor Authentication* (2FA) atau *Multi-Factor Authentication* (MFA), proses autentikasi memerlukan dua atau lebih bukti identitas, seperti kata sandi (faktor pengetahuan), kode OTP (faktor kepemilikan), atau biometrik (faktor inheren). Ini meningkatkan keamanan secara signifikan dibandingkan autentikasi satu faktor karena jika satu faktor diretas, faktor lain tetap melindungi akses. Dalam konteks perlindungan data pribadi, MFA mencegah akses tidak sah, kebocoran, atau penyalahgunaan Data, terutama dalam lingkungan yang rawan ancaman siber.

- c. Audit trail untuk mencatat setiap aktivitas Pemrosesan Data.
Audit trail sangat penting dalam perlindungan data pribadi karena mencatat setiap aktivitas Pemrosesan Data, termasuk siapa yang mengakses, kapan, dan untuk tujuan apa. Dengan audit trail, transparansi dan akuntabilitas dapat terjaga, memastikan setiap tindakan terhadap DTSEN terdokumentasi dengan jelas. Ini membantu mendeteksi aktivitas mencurigakan, menyelidiki insiden kebocoran Data, serta mematuhi regulasi keamanan dan perlindungan Data pribadi. Audit trail juga berfungsi sebagai alat verifikasi untuk memastikan sistem berjalan sesuai kebijakan, sekaligus memberikan bukti konkret dalam kasus pelanggaran atau sengketa terkait DTSEN.
- d. *Approval System*
Approval system sangat penting dalam pemrosesan Data, terutama untuk aktivitas yang memperlihatkan Data secara masif, baik di aplikasi maupun untuk kebutuhan dicetak. Dengan mekanisme persetujuan ini, setiap permintaan akses atau pemrosesan Data harus melalui verifikasi dan persetujuan pihak berwenang. Hal ini memastikan bahwa hanya pihak yang berhak dengan tujuan yang jelas yang dapat mengakses atau menampilkan DTSEN. *Approval system* mencegah penyalahgunaan, kebocoran, atau akses yang tidak sah, serta meningkatkan kontrol, akuntabilitas, dan kepatuhan terhadap regulasi keamanan dan perlindungan Data pribadi. *Approval System* ini diklasifikasikan berdasarkan risiko, mana yang perlu *approval* biasa dan *approval* yang membutuhkan Tanda Tangan Elektronik.
- e. TTE
TTE sangat penting dalam sistem *approval* untuk pengelolaan DTSEN karena memastikan keaslian, integritas, dan *non-repudiation* dari setiap persetujuan atau aktivitas pemrosesan Data. TTE memberikan bukti yang sah bahwa pihak yang memberikan persetujuan adalah benar dan terverifikasi, mencegah manipulasi atau penyalahgunaan Data. Dengan menggunakan teknologi kriptografi, TTE menjamin bahwa Data yang disetujui tidak diubah setelah ditandatangani. Hal ini juga membantu meningkatkan transparansi, akuntabilitas, serta memenuhi persyaratan hukum terkait keamanan dan perlindungan Data pribadi, terutama dalam aktivitas yang melibatkan akses, transfer, atau pemrosesan Data yang sensitif.

3. Teknik Pelindungan DTSEN

Berbagipakai Data terutama DTSEN menjadi kebutuhan mendesak dalam mendukung pelayanan publik yang efektif, transparan, dan akuntabel. Namun, tetap memprioritaskan perlindungan privasi individu sesuai dengan prinsip etika, peraturan, dan standar keamanan yang berlaku. Untuk itu, pedoman berbagipakai DTSEN ini menetapkan beberapa prinsip dasar teknik perlindungan Data untuk klasifikasi Data terbatas sebagai berikut.

a. *Anonimisasi*

Anonimisasi adalah proses menghilangkan informasi pengenalan secara permanen dari dataset, sehingga Data tidak dapat dikaitkan kembali dengan individu yang bersangkutan.

Prinsip ini penting untuk memastikan privasi dalam berbagi Data yang tidak memerlukan identifikasi langsung. Contoh penerapannya:

- 1) Menghapus nama, alamat, nomor identitas, dan informasi pribadi lainnya.
- 2) Menyediakan Data yang hanya berupa agregat, seperti statistik populasi atau distribusi demografis.

Contoh Penerapan Anonimisasi dalam DTSEN, sebuah Instansi Pusat ingin membagikan Data penerima bantuan sosial kepada lembaga riset untuk menganalisis efektivitas program. Sebelum dibagikan, Data harus dianonimkan dengan menghapus elemen pengenalan langsung seperti berikut:

Data Sebelum Anonimisasi:

ID Penerima	Nama	NIK	Alamat	Penghasilan	Jumlah Bantuan
1001	Agus Santoso	3200*****0001	Jl. Melati No. 5, Jakarta	1.500.000	600.000
1002	Siti Rahma	3200*****0001	Jl. Mawar No. 7, Bandung	1.200.000	750.000

Tabel 5.1 Contoh Data Sebelum *Anonimisasi*

Data setelah Anonimisasi:

ID Penerima	Wilayah	Kategori Penghasilan	Jumlah Bantuan
A001	Jakarta	< 2.000.000	600.000
A002	Bandung	< 2.000.000	750.000

Tabel 5.2 Contoh Data Setelah *Anonimisasi*

b. *Pseudonim*

Pseudonim adalah proses mengganti elemen pengenalan dalam dataset dengan nilai lain, seperti kode unik, sehingga Data tetap dapat dihubungkan kembali ke individu tertentu hanya dengan menggunakan kunci terpisah. Teknik ini memungkinkan analisis lanjutan tanpa membahayakan privasi. Contoh penerapannya:

- 1) Mengganti nama individu dengan ID unik yang disimpan secara terpisah.
- 2) Digunakan dalam analisis dataset longitudinal untuk pelacakan pola tanpa mengungkap identitas asli.

Dengan menggunakan Data sampel Anonimisasi, berikut penerapan *Pseudonim*:

ID Pseudonim	Wilayah	Kategori Penghasilan	Jumlah Bantuan
PZ-001	Jakarta	< 2.000.000	600.000
PZ-002	Bandung	< 2.000.000	750.000

Tabel 5.3 Contoh Data Setelah *Pseudonim*

Kunci yang menghubungkan ID *Pseudonim* dengan Identitas Asli disimpan secara terpisah dalam sistem yang aman.

c. *Masking*

Masking adalah teknik menyembunyikan sebagian atau seluruh elemen Data sensitif, biasanya dengan mengganti elemen tersebut dengan karakter acak atau simbol. Teknik ini sering digunakan untuk Data yang akan diproses atau dibagikan sementara, seperti:

- 1) Menampilkan sebagian nomor NIK (misalnya, 1234-****-789).
- 2) Menyembunyikan alamat email dengan tanda bintang (nama.pengguna@*.com).

ID Pseudonim	Nama	NIK
PZ-001	Agus Santoso	3200*****0001
PZ-002	Siti Rahma	3200*****0001

Tabel 5.4 Contoh Data Setelah *Masking*

d. *Minimasi*

Minimasi Data merupakan salah satu pilar penting dalam tata kelola berbagipakai Data yang bertanggung jawab. Minimasi ini menegaskan bahwa hanya Data yang relevan, esensial, dan sesuai dengan tujuan yang ditentukan yang boleh dikumpulkan, digunakan, dan dibagikan. Dengan menerapkan prinsip ini, instansi dapat mengurangi risiko kebocoran Data, penyalahgunaan, dan pelanggaran privasi.

- 1) Pentingnya Pembatasan pada Data yang Dibagikan. Prinsip minimisasi Data memastikan bahwa Data yang dibagi pakai tidak berlebihan atau di luar cakupan tujuan pengolahan. Sebelum memulai proses berbagipakai Data, Pengelola Data harus:
 - a) Melakukan evaluasi untuk menentukan Data apa yang benar-benar diperlukan.
 - b) Membatasi koleksi Data hanya pada informasi yang secara langsung mendukung tujuan yang telah dijelaskan.
 - c) Menghindari pengumpulan atau transfer Data tambahan yang tidak relevan.
Misalnya, jika tujuan berbagipakai Data adalah untuk analisis statistik, maka Data yang diidentifikasi secara pribadi (*personally identifiable information/PII*) harus dihapus atau dianonimkan sejauh mungkin.
- 2) Proses Penyaringan dan Validasi Pengelola Data harus menerapkan prosedur penyaringan dan validasi Data sebelum transfer dilakukan. Langkah ini melibatkan:
 - a) Identifikasi Data yang Relevan: Mengklasifikasikan Data berdasarkan relevansinya dengan tujuan transfer.
 - b) Penghapusan Data yang Tidak Diperlukan: Menghapus Data yang bersifat sensitif atau tidak relevan untuk meminimalkan risiko dan memastikan kepatuhan terhadap regulasi privasi.

- c) Agregasi atau Anonimisasi: Di mana memungkinkan, Data harus diolah menjadi bentuk agregat atau anonim untuk melindungi identitas individu.

e. *Access Control*

Prinsip kontrol akses menetapkan bahwa hanya pihak yang berwenang yang dapat mengakses Data berdasarkan kebutuhan spesifik dan hak akses yang telah ditentukan. Contoh penerapannya:

- 1) Implementasi autentikasi berbasis peran (*Role-Based Access Control* - RBAC).
- 2) Memastikan Data hanya dapat diakses oleh pengguna terotorisasi untuk tujuan yang ditentukan.

f. *Akuntabilitas*

Prinsip akuntabilitas merupakan pondasi dalam tata kelola berbagipakai Data yang bertujuan untuk memastikan bahwa semua pihak yang terlibat memiliki tanggung jawab yang jelas dan dapat dipertanggungjawabkan. Akuntabilitas tidak hanya mencakup tanggung jawab legal tetapi juga mencakup aspek etis dan operasional dalam mengelola dan melindungi Data selama proses pertukaran.

- 1) Penetapan Peran dan Tanggung Jawab dalam setiap proses pertukaran Data, penting untuk menetapkan peran dan tanggung jawab yang spesifik bagi semua pihak yang terlibat. Hal ini mencakup:
 - a) Pengendali Data (*Data Controller*): Bertanggung jawab untuk menentukan tujuan dan sarana pemrosesan Data, termasuk memastikan bahwa semua aktivitas pertukaran Data mematuhi regulasi yang berlaku.
 - b) Prosesor Data (*Data Processor*): Bertanggung jawab untuk memproses Data sesuai dengan instruksi dari pengendali Data, serta memastikan keamanan Data selama proses tersebut.

Setiap pihak juga harus memastikan adanya mekanisme untuk menangani pelanggaran atau keluhan dari Subjek Data Pribadi secara efektif.

- 2) Dokumentasi dan Transparansi Akuntabilitas menuntut bahwa setiap tindakan dalam proses pertukaran Data terdokumentasi dengan baik. Dokumentasi ini mencakup:
 - a) Kebijakan dan prosedur terkait pertukaran Data.
 - b) Catatan aktivitas transfer Data, termasuk informasi tentang pihak-pihak yang terlibat, waktu transfer, dan tujuan transfer.
 - c) Perjanjian formal, seperti Perjanjian Kerja Sama (PKS) atau *Non-Disclosure Agreement* atau berita acara serah terima atau kontrak yang menjabarkan tanggung jawab masing-masing pihak.

Dokumentasi yang baik memungkinkan pengelola Data untuk membuktikan kepatuhan terhadap regulasi dan mengatasi potensi perselisihan.

- 3) Pengawasan dan Audit Untuk memastikan akuntabilitas, pengawasan dan audit berkala harus dilakukan. Hal ini mencakup:

- a) Audit Internal: Dilakukan untuk menilai kepatuhan terhadap kebijakan internal dan regulasi eksternal.
- b) Audit Eksternal: Pihak ketiga independen dapat dilibatkan untuk memeriksa proses pertukaran Data dan memberikan rekomendasi perbaikan.
- c) Pemantauan *Real-Time*: Penggunaan teknologi untuk memantau aktivitas transfer Data secara langsung dan mendeteksi anomali atau pelanggaran.
- 4) Mekanisme Penanganan Insiden dalam situasi di mana terjadi pelanggaran Data, akuntabilitas berarti memiliki mekanisme yang jelas untuk menanggapi insiden tersebut. Hal ini mencakup:
 - a) Identifikasi dan mitigasi risiko secepat mungkin.
 - b) Pemberitahuan kepada pengelola DTSEN dan otoritas yang relevan sesuai regulasi.
 - c) Langkah-langkah korektif untuk mencegah insiden serupa di masa depan.
- 5) Pendidikan dan Kesadaran Akuntabilitas juga mencakup tanggung jawab untuk memastikan bahwa semua personil yang terlibat dalam pertukaran Data memiliki pemahaman yang memadai tentang kebijakan, prosedur, dan tanggung jawab mereka. Pelatihan yang berkelanjutan harus diberikan untuk menjaga kepatuhan dan memperkuat budaya akuntabilitas.

4. Penggunaan Infrastruktur SPBE

Sistem layanan berbagipakai DTSEN merupakan aplikasi yang termasuk dalam SPBE dan harus mengikuti pedoman yang diatur dalam Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Mengacu pada Peraturan Presiden tersebut, setiap aplikasi SPBE wajib menggunakan infrastruktur SPBE yang telah ditetapkan. Infrastruktur SPBE mencakup ekosistem PDN, JIP, dan SPLP.

Penggunaan SPLP bertujuan untuk memudahkan integrasi antar layanan SPBE di berbagai instansi. Dalam menggunakan SPLP, Instansi Pusat dan Pemerintah Daerah (IPPD) diwajibkan untuk membangun keterhubungan dan akses antara Jaringan Intra IPPD dengan JIP. JIP adalah jaringan interkoneksi tertutup yang menghubungkan jaringan intra antar instansi pusat dan pemerintah daerah.

JIP berperan penting untuk memastikan bahwa semua transaksi Data antar Instansi Pusat, baik di tingkat pusat maupun daerah, dilakukan dengan aman. Keamanan menjadi prioritas utama untuk mencegah kebocoran atau penyalahgunaan Data. Jaringan JIP ini bersifat tertutup guna memastikan bahwa Data yang dibagikan antar instansi pemerintah tetap terjaga integritasnya dan aman dari ancaman eksternal.

BAB VI PEMANTAUAN DAN EVALUASI

A. Pemantauan dan Evaluasi Berkala Pemanfaatan DTSEN

Pengendali DTSEN melakukan pemantauan dan evaluasi berkala terhadap pemanfaatan DTSEN memastikan bahwa Data yang dikumpulkan dan digunakan oleh organisasi dikelola secara efektif dan sesuai dengan peraturan yang berlaku. Diantara aspek dalam pemantauan antara lain *traffic monitoring*, *crawling*, hak akses.

Traffic monitoring meliputi pemantauan aliran Data untuk mengidentifikasi pola penggunaan dan potensi penyalahgunaan. Dengan melakukan *traffic monitoring*, organisasi dapat mendeteksi aktivitas mencurigakan, seperti akses tidak sah atau penggunaan Data di luar tujuan yang telah ditentukan. Hal ini penting untuk mencegah kebocoran Data dan memastikan bahwa DTSEN tetap terlindungi dari ancaman siber yang semakin kompleks di era digital saat ini.

Crawling adalah proses yang melibatkan pengumpulan informasi dari berbagai sumber di internet, yang dapat mencakup DTSEN. Oleh karena itu, penting bagi organisasi untuk menerapkan kebijakan yang jelas mengenai *crawling*, termasuk batasan-batasan dalam pengumpulan Data dan cara penyimpanannya. Dengan adanya kebijakan yang ketat, organisasi dapat meminimalkan risiko penyalahgunaan Data dan memastikan bahwa semua aktivitas *crawling* dilakukan dengan izin yang tepat dari Subjek Data Pribadi. Selain itu, akses Data oleh pihak ketiga harus diawasi secara ketat untuk mencegah potensi pelanggaran privasi.

Hak akses juga termasuk dalam penilaian pemantauan dan evaluasi berkala. Organisasi perlu memastikan bahwa hanya individu atau entitas berwenang yang memiliki hak akses ke DTSEN. Ini dapat dicapai melalui penerapan kontrol akses yang ketat dan audit rutin untuk menilai kepatuhan terhadap kebijakan yang disepakati antar pihak terkait.

B. Pelaksana Pemantauan dan Evaluasi Pemanfaatan DTSEN

Pelaksana pemantauan dan evaluasi ini terdiri dari berbagai pemangku kepentingan, termasuk perwakilan dari departemen hukum, TI, dan keamanan informasi, serta anggota independen yang memiliki keahlian dalam perlindungan Data.

Pelaksana pemantauan dan evaluasi pemanfaatan Data menjalankan fungsi pengawasan dan evaluasi dalam menilai efektivitas dan kepatuhan terhadap kebijakan perlindungan DTSEN dalam suatu organisasi sekaligus penasihat strategis dalam mengelola risiko terkait perlindungan Data. Tugas pelaksana pemantauan dan evaluasi terhadap pemanfaatan Data adalah sebagai berikut.

1. Melakukan pengendalian berkala terhadap pengelolaan DTSEN;
2. Memastikan aktivitas pemrosesan DTSEN dilakukan sesuai dengan ketentuan peraturan perundang-undangan;
3. Melakukan evaluasi dampak pemanfaatan DTSEN; dan
4. Memastikan Portal SDI dan/atau portal/sistem informasi yang dikelola oleh Pengendali DTSEN sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

BAB VII GLOSARIUM

DTSEN

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

Pengendali Data (*Data Controller*)

Setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan DTSEN.

Prosesor Data (*Data Processor*)

Setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan DTSEN atas nama Pengendali DTSEN.

Subjek Data Pribadi

Orang perorangan yang pada dirinya melekat DTSEN.

Pejabat/Petugas Pelindungan Data (*Data Protection Officer - DPO*)

Orang yang ditunjuk untuk memastikan bahwa pengelolaan DTSEN sesuai dengan peraturan yang berlaku dan melindungi hak-hak Subjek Data Pribadi.

Penyelenggara Sistem Elektronik (PSE)

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.

Pusat Data Nasional

Sekumpulan Pusat Data yang digunakan secara bagipakai oleh Instansi Pusat dan Pemerintah Daerah dan saling terhubung

Identifikasi Risiko

Proses mengenali potensi ancaman dan kerentanan yang dapat mempengaruhi keamanan Data.

Mitigasi Risiko

Tindakan teknis dan operasional yang diambil untuk mengurangi atau mengelola risiko yang diidentifikasi.

Penanganan Insiden Keamanan

Proses untuk merespons dan mengelola insiden keamanan seperti pelanggaran Data, termasuk deteksi, mitigasi, dan pelaporan.

Klasifikasi Data

Proses mengelompokkan Data berdasarkan tingkat sensitivitas, pentingnya Data, dan dampaknya terhadap keamanan.

Audit dan Monitoring Keamanan

Proses penilaian sistem keamanan secara berkala untuk memastikan bahwa Data dilindungi sesuai dengan standar yang berlaku.

Permintaan Data

Proses pengajuan permintaan akses Data oleh pihak yang berkepentingan sesuai prosedur yang ditetapkan.

Validasi Administrasi

Pemeriksaan kelengkapan dan keabsahan dokumen yang diperlukan untuk memproses permintaan Data.

Proses Pemrosesan Data

Aktivitas pengolahan Data dari pengumpulan hingga penyajian sesuai dengan kebutuhan yang ditetapkan.

Penyerahan Data

Proses mengirimkan Data yang telah diproses kepada pihak yang berhak menerima berdasarkan perjanjian atau peraturan yang berlaku.

Pemanfaatan Data

Penggunaan Data untuk tujuan tertentu yang telah disepakati, seperti penelitian, pengambilan keputusan, atau layanan publik.

Pemantauan Berkala

Proses penilaian berkala terhadap efektivitas pengelolaan dan keamanan Data.

Hak Akses Data

Hak yang diberikan kepada pengguna atau organisasi untuk mengakses Data tertentu sesuai dengan tingkat kewenangan yang dimiliki.

Pelatihan Keamanan Data

Pelatihan yang diberikan untuk meningkatkan kemampuan teknis dan kesadaran staf dalam mengelola Data secara aman dan sesuai peraturan.

Perjanjian Pemrosesan Data (*Data Processing Agreement* - DPA)

Kesepakatan antara Pengendali Data dan Prosesor Data yang mengatur tanggung jawab dan kewajiban terkait pemrosesan DTSEN.

Subjek Data (*Data Owner*)

Pihak yang memiliki otoritas penuh atas Data tertentu dan bertanggung jawab untuk menetapkan kebijakan penggunaan dan keamanan Data tersebut.

Data Induk

Data yang merepresentasikan objek dalam proses bisnis pemerintah yang ditetapkan sesuai dengan ketentuan perundangan.

Data Terbuka

Data hasil dari pengelompokan, penggabungan, atau perhitungan dari Data tingkat individu atau keluarga menjadi bentuk yang lebih umum atau ringkasan untuk tingkat nasional/ provinsi/ kabupaten/ kota.

Data Terbatas

Data tingkat individu atau keluarga tanpa dilengkapi variabel terkait identitas (telah dilakukan de-identifikasi) untuk tingkat nasional/provinsi/kabupaten/kota. Variabel terkait identitas termasuk namun tidak terbatas pada nama, Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK), alamat, dan koordinat geografis tempat tinggal.

Data Tertutup

Data tingkat individu atau keluarga dilengkapi dengan variabel terkait identitas untuk Tingkat nasional/provinsi/kabupaten/kota/desa/kelurahan. Variabel terkait identitas termasuk namun tidak terbatas pada nama, Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK), alamat, dan koordinat geografis tempat tinggal.

Enkripsi Data

Proses mengamankan Data dengan mengubahnya menjadi format yang tidak dapat dibaca tanpa kunci dekripsi.

Autentikasi Multifaktor (MFA)

Metode keamanan yang memerlukan lebih dari satu bentuk verifikasi untuk mengakses Data atau sistem

Sistem Deteksi Intrusi (IDS)

Sistem keamanan yang memonitor jaringan untuk mendeteksi aktivitas mencurigakan atau pelanggaran keamanan.

Protokol Transfer Aman (SFTP, TLS)

Protokol jaringan yang digunakan untuk mentransfer Data secara aman melalui internet dengan menggunakan enkripsi.

MENTERI PERENCANAAN
PEMBANGUNAN NASIONAL/
KEPALA BADAN
PERENCANAAN
PEMBANGUNAN NASIONAL,

ttd.

RACHMAT PAMBUDY