URAIAN KONDISI EXISTING TATA KELOLA PELINDUNGAN DATA PRIBADI (PDP)

1. Gambaran Umum

Dinas Komunikasi dan Informatika Kota Pekalongan telah menerapkan tata kelola keamanan informasi melalui penerapan Sistem Manajemen Keamanan Informasi (SMKI), pembentukan Tim SMKI, penerapan kebijakan keamanan informasi, pelaksanaan manajemen risiko, audit internal, dan pengelolaan keamanan SPBE. Tata kelola tersebut menjadi fondasi awal bagi pengembangan tata kelola Pelindungan Data Pribadi (PDP) di lingkungan organisasi.

Organisasi juga telah memasukkan aspek Pelindungan Data Pribadi ke dalam kebijakan keamanan informasi melalui Bab XV Pengendalian Pelindungan Data Pribadi pada Kebijakan Teknis SMKI v2.0.pdf. Kebijakan tersebut telah memuat prinsip pelindungan data pribadi, hak subjek data pribadi, pemrosesan data pribadi, dan penanganan insiden PDP.

2. Kondisi Existing Tata Kelola PDP

2.1 Organisasi dan Penanggung Jawab PDP

Berdasarkan dokumen SK Kadinkominfo 500.12.10-270 Tahun 2025 tentang Pembentukan Tim SMKI Dinas Kominfo Kota Pekalongan.pdf, organisasi telah membentuk Tim SMKI yang didalamnya terdapat fungsi yang mendukung pelaksanaan Pelindungan Data Pribadi, termasuk keberadaan Koordinator Pelindungan Data Pribadi, Koordinator Kepatuhan Hukum, Koordinator Manajemen Risiko, dan Koordinator Manajemen Insiden.

Namun demikian, organisasi belum memiliki penetapan formal **Pejabat/Petugas Pelindungan Data Pribadi (PPDP/DPO)** sebagaimana diamanatkan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Fungsi PDP masih dijalankan sebagai bagian dari struktur SMKI dan belum berdiri sebagai fungsi kepatuhan PDP yang khusus.

2.2 Kebijakan dan Dokumen PDP

Organisasi telah memiliki beberapa dokumen yang mendukung tata kelola PDP, antara lain:

- Kebijakan Umum SMKI;
- Kebijakan Teknis SMKI;
- Pedoman Manajemen Risiko SPBE;
- Risk Register SPBE;
- Ketentuan pengendalian akses;
- Pengendalian kriptografi dan data masking;

- Pengendalian pelindungan data pribadi pada SMKI.

Meski demikian, organisasi belum memiliki:

- Kebijakan Pelindungan Data Pribadi yang berdiri sendiri;
- Pedoman tata kelola PDP;
- SOP hak subjek data pribadi;
- Standar Privacy Notice organisasi;
- Record of Processing Activities (RoPA);
- Data Protection Impact Assessment (DPIA).

2.3 Awareness dan Kompetensi PDP

Organisasi telah melaksanakan awareness keamanan informasi melalui kegiatan pelatihan ISO/IEC 27001:2022 bagi pegawai. Materi tersebut telah mengenalkan regulasi keamanan informasi dan pelindungan data pribadi.

Namun belum tersedia:

- program awareness PDP yang terstruktur;
- kurikulum kompetensi PDP;
- pelatihan khusus PDP;
- sertifikasi PPDP/DPO.

2.4 Mekanisme Hak Subjek Data

Hak-hak Subjek Data Pribadi telah diatur pada kebijakan internal SMKI. Namun pelaksanaannya masih menggunakan mekanisme layanan umum dan belum tersedia:

- kanal khusus hak subjek data;
- SOP layanan hak subjek data;
- sistem pencatatan permohonan;
- monitoring layanan hak subjek data.

2.5 Privacy Notice dan Transparansi Pemrosesan Data

Organisasi telah mulai menerapkan transparansi pemrosesan data melalui:

- halaman kebijakan privasi pada portal Pemerintah Kota Pekalongan;

- dokumen persetujuan pada beberapa layanan digital.

Namun penerapan tersebut belum:

- mencakup seluruh layanan digital;
- menggunakan format standar yang sama;
- dikelola melalui mekanisme review berkala;
- didukung inventarisasi layanan yang memproses data pribadi.

2.6 Pengelolaan Risiko PDP

Organisasi telah memiliki Pedoman Manajemen Risiko SPBE dan Risk Register SPBE yang mengidentifikasi berbagai risiko keamanan informasi. Beberapa risiko terkait data pribadi juga telah mulai teridentifikasi, seperti:

- insiden pencurian data pribadi;
- kesalahan pengelolaan informasi terbatas;
- penyalahgunaan hak akses;
- kebocoran data akibat human error.

Namun sampai saat ini belum tersedia:

- Risk Register PDP;
- DPIA;
- metodologi khusus risiko PDP;
- monitoring risiko PDP secara terpisah.

2.7 Pengamanan Data Pribadi

Organisasi telah menerapkan berbagai pengamanan teknis melalui SMKI, antara lain:

- pengendalian akses;
- autentikasi pengguna;
- klasifikasi informasi;
- logging dan monitoring;
- backup data;
- kriptografi;

- data masking;
- pengelolaan insiden keamanan informasi;
- pengamanan jaringan dan aplikasi.

Pengamanan tersebut telah mendukung perlindungan data pribadi, namun belum dilakukan pemetaan dan evaluasi secara khusus terhadap seluruh siklus hidup data pribadi yang diproses pada layanan digital pemerintah.

HASIL IDENTIFIKASI KEBUTUHAN TATA KELOLA PDP

Berdasarkan kondisi existing, diidentifikasi kebutuhan penguatan tata kelola PDP sebagai berikut:

No	Area	Kebutuhan
1	Organisasi	Penetapan PPDP/DPO melalui SK Kepala Dinas
2	Tata Kelola	Penyusunan kebijakan PDP yang berdiri sendiri
3	Data	Inventarisasi sistem dan layanan yang memproses data pribadi
4	Pemrosesan Data	Penyusunan Record of Processing Activities (RoPA)
5	Risiko	Pelaksanaan DPIA dan penyusunan Risk Register PDP
6	Hak Subjek Data	Penyusunan SOP, formulir, dan kanal khusus layanan hak subjek data
7	Privacy Notice	Standardisasi dan penerapan Privacy Notice pada seluruh layanan digital
8	SDM	Program awareness dan kompetensi PDP
9	Monitoring	Mekanisme monitoring kepatuhan PDP
10	Implementasi	Penyusunan Roadmap dan Rencana Aksi Implementasi PDP

Kesimpulan

Berdasarkan hasil inventarisasi, Dinas Komunikasi dan Informatika Kota Pekalongan telah memiliki fondasi tata kelola yang mendukung Pelindungan Data Pribadi melalui penerapan SMKI, pembentukan Tim SMKI, keberadaan Koordinator PDP, kebijakan keamanan informasi, pelaksanaan manajemen risiko, serta berbagai kontrol keamanan teknis. Selain itu, aspek PDP

telah mulai diakomodasi dalam kebijakan internal dan sebagian layanan digital telah menerapkan kebijakan privasi.

Namun tata kelola PDP masih berada pada tahap perintisan karena belum terdapat PPDP/DPO yang ditetapkan secara formal, belum tersedia tata kelola PDP yang komprehensif, belum dilakukan inventarisasi pemrosesan data pribadi secara menyeluruh, belum tersedia mekanisme hak subjek data yang terstruktur, belum dilakukan DPIA, dan belum tersedia Risk Register PDP. Oleh karena itu diperlukan penyusunan rencana aksi implementasi PDP sebagai dasar peningkatan tingkat kematangan PDP menuju level berikutnya.

PEMERINTAH KOTA PEKALONGAN
DINAS KOMUNIKASI DAN INFORMATIKA

KEBIJAKAN TEKNIS SISTEM MANAJEMEN KEAMANAN INFORMASI

Nomor Dokumen	000.6/379
Versi	2.0
Tanggal Berlaku Efektif	25 Agustus 2024
Klasifikasi	Internal
Pemilik Dokumen	Tim SMKI

Halaman Pengesahan

Disetujui Oleh:	**ARIF KARYADI S.Sos.** Kepala Dinas Komunikasi dan Informatika
Diketahui Oleh:	**ROFIEQ, SH** Sekretaris Dinas Komunikasi dan Informatika
Diperiksa Oleh:	**Dr. KUSUMA ADI ACHMAD S.E., M.T.** Kepala Bidang Aplikasi dan Persandian selaku CISO
Disusun Oleh:	**MEIDY PRASETYO UTOMO, S.Kom** Kepala Seksi Persandian dan Keamanan Informasi selaku Tim SMKI

Riwayat Perubahan Dokumen

Versi	Tanggal Revisi	Uraian Perubahan	Penyusun
1.0	25/01/2023	Terbitan Awal	Tim SMKI
2.0	22/08/2024	- Penambahan Halaman Pengesahan - Riwayat Perubahan Dokumen - Penambahan pengendalian penyamaran data di bagian Pengendalian Kriptografi - Penambahan pengendalian Pelindungan Data Pribadi - Penambahan pengendalian Pelindungan Data Pribadi - Penambahan Intelijen Ancaman (Threat Intelligence) - Penambahan pengendalian Keamanan Informasi Layanan Cloud - Penambahan pengendalian Manajemen Konfigurasi - Penambahan Penyaringan Website	Meidy

Daftar Isi

1. Pengendalian Dokumen 7
1.1. Tujuan 7
1.2. Ruang Lingkup 7
1.3. Kebijakan 8
1.4. Standar 9
2. Pengendalian Organisasi Keamanan Informasi 13
2.1. Tujuan 13
2.2. Ruang Lingkup 13
2.3. Kebijakan 13
2.4. Standar 15
3. Keamanan Sumber Daya Manusia 21
3.1. Tujuan 21
3.2. Ruang Lingkup 21
3.3. Kebijakan 21
3.4. Standar 22
4. Pengendalian dan Pengelolaan Aset Informasi 24
4.1. Tujuan 24
4.2. Ruang Lingkup 24
4.3. Kebijakan 24
4.9. Standar 26
5. Pengendalian Akses 28
5.1. Tujuan 28
5.2. Ruang Lingkup 28
5.3. Kebijakan 28
5.4. Standar 32
6. Pengendalian terhadap Penerapan Kriptografi dan Penyamanan Data (Data Masking) 35
6.1. Tujuan 35
6.2. Ruang Lingkup 35
6.3. Kebijakan 35
6.4. Standar 36
7. Pengendalian dan Pengelolaan Keamanan Fisik dan Lingkungan 38
7.1. Tujuan 38
7.2. Ruang Lingkup 38
7.3. Kebijakan 38
7.4. Standar 40
8. Pengendalian dan Pengelolaan Keamanan Operasional 44

8.1. Tujuan 44
8.2. Ruang Lingkup 44
8.3. Kebijakan 44
8.4. Standar 48
9. Pengendalian Keamanan Komunikasi 52
9.1. Tujuan 52
9.2. Ruang Lingkup 52
9.3. Kebijakan 52
9.4. Standar 53
10. Pengendalian Keamanan Informasi dalam Akuisisi, Pengembangan dan Perawatan Sistem Informasi 57
10.1. Tujuan 57
10.2. Ruang Lingkup 57
10.3. Kebijakan 57
10.4. Standar 59
11. Pengendalian Hubungan dengan Pihak Ketiga atau Pemasok 65
11.1. Tujuan 65
11.2. Ruang Lingkup 65
11.3. Kebijakan 65
11.4. Standar 66
12. Pengendalian dan Pengelolaan Gangguan Keamanan Informasi 67
12.1. Tujuan 67
12.2. Ruang Lingkup 67
12.3. Kebijakan 67
12.4. Standar 68
13. Pengendalian Aspek Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan 71
13.1. Tujuan 71
13.2. Ruang Lingkup 71
13.3. Kebijakan 71
13.4. Standar 72
14. Pengendalian Kepatuhan 75
14.1. Tujuan 75
14.2. Ruang Lingkup 75
14.3. Kebijakan 75
14.4. Standar 77
15. Pengendalian Pelindungan Data Pribadi 79
15.1. Tujuan 79
15.2. Ruang Lingkup 79

15. Pengendalian Pelindungan Data Pribadi

15.1. Tujuan

Pengendalian pelindungan data pribadi dirancang untuk memastikan bahwa data pribadi yang ditangani oleh Dinas Komunikasi dan Informatika dilindungi secara efektif dari akses yang tidak sah, penggunaan yang tidak sah, atau kebocoran yang tidak disengaja. Selain itu, untuk memastikan kepatuhan terhadap peraturan perundang-undangan terkait dengan Pelindungan Data Pribadi yang berlaku serta membangun kepercayaan Subjek Data Pribadi

15.2. Ruang Lingkup

15.2.1. Kepatuhan terhadap peraturan perundangan yang terkait pelindungan data pribadi

15.2.2. Pelindungan Data Pribadi yang ditangani

15.3. Kebijakan

15.3.1. Pemrosesan Data Pribadi

a. Kegiatan pemrosesan data pribadi meliputi pemerolehan, pengumpulan, tujuan penggunaan, pengolahan, penganalisisan, penyimpanan, perbaikan, pembaruan, penampilan, pengumuman, transfer, penyebarluasan, pengungkapan, dan/atau penghapusan atau pemusnahan.

b. Pemrosesan data pribadi harus dilakukan sesuai dengan Prinsip Pelindungan Data Pribadi.

c. Apabila pemrosesan data pribadi dilakukan dengan melibatkan pihak ketiga/vendor maka minimal harus terdapat perjanjian yang memuat peran, tanggung jawab, dan hubungan antara organisasi dengan pihak ketiga/vendor, memiliki tujuan yang saling berkaitan dan cara pemrosesan Data Pribadi yang ditentukan secara bersama, serta terdapat narahubung yang ditunjuk secara bersama-sama.

d. Organisasi yang melakukan pemrosesan Data Pribadi harus mendapatkan persetujuan yang sah secara eksplisit dari Subjek Data Pribadi untuk satu atau beberapa tujuan tertentu yang telah disampaikan oleh organisasi kepada Subjek Data Pribadi.
e. Di dalam persetujuan tersebut, organisasi harus menyampaikan informasi terkait legalitas, tujuan, dan jangka waktu pemrosesan Data Pribadi, jenis dan relevansi Data Pribadi yang akan diproses, jangka waktu retensi dokumen yang memuat Data Pribadi, rincian mengenai informasi yang dikumpulkan, dan hak Subjek Data Pribadi.
f. Persetujuan pemrosesan Data Pribadi dilakukan melalui persetujuan tertulis atau terekam, baik disampaikan secara elektronik maupun non-elektronik.
g. Persetujuan tersebut harus disampaikan dengan bahasa yang sederhana, jelas, dapat dipahami, mudah diakses, dan dapat dibedakan secara jelas dengan hal lainnya.
h. Organisasi yang melakukan pemrosesan Data Pribadi harus melakukan verifikasi untuk memastikan keakuratan, kelengkapan, dan konsistensi Data Pribadi sesuai dengan Peraturan Perundang-undangan.
i. Pemrosesan Data Pribadi wajib diakhiri apabila telah mencapai masa retensi, tujuan pemrosesan Data Pribadi telah tercapai, atau terdapat permintaan dari Subjek Data Pribadi.
j. Pengendali Data Pribadi wajib melakukan perekaman terhadap seluruh kegiatan pemrosesan Data Pribadi.

15.3.2. Prinsip Pelindungan Data Pribadi

a. Pengumpulan Data Pribadi dilakukan secara terbatas, spesifik, sah secara hukum, dan transparan.
b. Pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya

c. Pemrosesan Data Pribadi dilakukan dengan menjamin hak Subjek Data Pribadi
d. Pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan
e. Pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari pengaksesan, pengungkapan, dan pengungkapan yang tidak sah, serta penyalahgunaan, perusakan dan/atau penghilangan Data Pribadi.
f. Pemrosesan Data Pribadi dilakukan secara bertanggung jawab dan dapat dibuktikan secara jelas

15.3.3. Hak Subjek Data Pribadi

Setiap Subjek Data Pribadi memiliki hak:

a. Mendapatkan informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan Data Pribadi, dan akuntabilitas pihak yang meminta Data Pribadi.
b. Melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi sesuai dengan tujuan pemrosesan Data Pribadi tentang dirinya.
c. Mendapatkan akses dan memperoleh salinan Data Pribadi tentang dirinya.
d. Mengakhiri pemrosesan, menghapus, dan/atau memusnahkan Data Pribadi tentang dirinya.
e. Menarik kembali persetujuan pemrosesan Data Pribadi tentang dirinya.
f. Menunda atau membatasi pemrosesan Data Pribadi.
g. Mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis.
h. Menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai undang-undang.

i. Mendapatkan dan/atau menggunakan Data Pribadi tentang dirinya dalam bentuk yang sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik.

15.3.4. Penanganan Insiden dan/atau Permohonan Hak Subjek Data Pribadi

a. Pelaksanaan atau permintaan hak Subjek Data Pribadi diajukan melalui permohonan tercatat yang dapat disampaikan secara elektronik atau nonelektronik oleh Subjek Data Pribadi kepada Pengendali Data Pribadi.
b. Pengendali Data Pribadi wajib memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi paling lambat 3x24 jam terhitung sejak Pengendali Data Pribadi menerima permintaan pembaruan dan/atau perbaikan Data Pribadi dari Subjek Data Pribadi. organisasi wajib memberitahukan hasil pembaruan dan/atau perbaikan Data Pribadi kepada Subjek Data Pribadi jika sudah selesai diperbaharui dan/atau diperbaiki.
c. Pengendali Data Pribadi wajib memberikan akses Data pribadi yang diproses serta rekam jejak pemrosesan Data Pribadi paling lambat 3x24 jam terhitung sejak Pengendali Data Pribadi menerima permintaan akses dari Subjek Data Pribadi.
d. Pengendali Data Pribadi wajib menghentikan pemrosesan Data Pribadi apabila Subjek Data Pribadi menarik kembali persetujuan pemrosesan Data Pribadi. Penghentian pemrosesan Data Pribadi tersebut wajib dilakukan 3x24 jam terhitung sejak Pengendali Data Pribadi menerima permintaan penarikan kembali persetujuan pemrosesan Data Pribadi dari Subjek Data Pribadi.
e. Pengendali Data Pribadi wajib melakukan penundaan dan pembatasan pemrosesan Data Pribadi baik sebagian maupun seluruhnya paling lambat 3x24 jam terhitung sejak Pengendali

Data Pribadi menerima permintaan penundaan dan pembatasan proses Data Pribadi

f. Apabil terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3x24 jam kepada:
   i. Subjek Data Pribadi; dan
   ii. Lembaga
g. Pemberitahuan tertulis sebagaimana dimaksud pada poin sebelumnya minimal, memuat:
   i. Data Pribadi yang terungkap;
   ii. kapan dan bagaimana Data Pribadi terungkap; dan
   iii. upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi.

15.3.5. Jenis-Jenis Data Pribadi yang Dikumpulkan

Data Pribadi merupakan data yang mengidentifikasi atau dapat digunakan untuk mengidentifikasi, menghubungi, atau menemukan orang atau perangkat yang terkait dengan data tersebut. Berdasarkan Peraturan Perundang-undangan yang berlaku, Data Pribadi terdiri dari Data Pribadi Umum dan spesifik/sensitif. Data Pribadi yang dikumpulkan dikategorikan sebagai berikut:

a. Data identitas termasuk nama, nama pengguna, kata sandi, kartu tanda penduduk, nomor pokok wajib pajak, identitas pengguna atau pengenal lainnya, jabatan, tanggal kelahiran, jenis kelamin, tempat kelahiran, pekerjaan, kebangsaan, foto dan/atau data biometrik.
b. Data kontak termasuk alamat penagihan, alamat pengiriman, alamat email, nomor telepon, dan daftar kontak.
c. Data kelayakan termasuk, dalam kaitannya dengan Penjual, seperti perizinan, persetujuan, dan detail polis asuransi.
d. Data Transaksi termasuk pembelian atau pesanan yang Anda lakukan, minat, preferensi, masukan, dan tanggapan survei Anda, sehubungan dengan Pengguna, jenis layanan yang

dicari, perincian mengenai pengambilan dan/atau pengiriman, dan jenis layanan yang dapat diterima pada saat itu.

e. Data Keuangan termasuk rincian rekening bank dan kartu pembayaran seperti jenis kartu atau rekening pembayaran yang digunakan, nama penerbit kartu atau rekening pembayaran tersebut, nama pemegang kartu atau rekening pembayaran tersebut, nomor identifikasi rekening tersebut atau kartu pembayaran, kode verifikasi kartu pembayaran atau akun tersebut, dan tanggal kadaluarsa kartu pembayaran atau akun tersebut, sebagaimana berlaku, data virtual account, riwayat keuangan (termasuk namun tidak terbatas pada riwayat transaksi kartu pembayaran atau rekening, rincian kartu pembayaran atau rekening, kode CVV dan pemetaan dan/atau status dan keadaan dari kartu pembayaran atau rekening), dan data penilaian kredit (credit scoring).

f. Data Pembayaran termasuk rincian pembayaran atau transfer yang dilakukan oleh Pengguna pada Aplikasi Kami, termasuk namun tidak terbatas pada data yang berkaitan dengan penggunaan, pembayaran, rincian penerima (termasuk rincian rekening mereka), metode pembayaran yang digunakan, jumlah pembayaran yang dibayarkan, rincian tagihan, dan rincian faktur.

g. Data Teknis termasuk rincian tentang penggunaan Anda atas Aplikasi Kami seperti identifikasi yang dihasilkan oleh Aplikasi (user id) alamat protokol internet (IP), data sebagai halaman web yang dilihat sebelumnya atau sesudahnya, durasi setiap kunjungan/sesi, identitas (ID) perangkat internet atau alamat kontrol akses media, ID periklanan dan informasi perangkat lainnya termasuk informasi mengenai produsen, model, dan sistem operasi perangkat yang Anda gunakan untuk mengakses Aplikasi dan crash logs.

h. Data Perangkat termasuk data perangkat, diantaranya jenis perangkat yang Anda gunakan untuk mengakses Aplikasi, termasuk model perangkat keras, sistem operasi dan versinya, perangkat lunak, nomor IMEI, nama file dan versinya, pilihan bahasa, pengenal perangkat unik, pengenal iklan, nomor seri, informasi gerakan perangkat, dan/atau informasi jaringan seluler.

i. Data Catatan (log) termasuk catatan pada server yang menerima data seperti alamat IP perangkat, tanggal dan waktu akses, fitur aplikasi atau laman yang dilihat, proses kerja aplikasi dan aktivitas sistem lainnya, jenis peramban (browser), dan/atau situs atau layanan pihak ketiga yang Pengguna gunakan sebelum berinteraksi dengan Aplikasi.

j. Data Lokasi termasuk data lokasi geografis waktu-nyata (real-time) Anda, titik koordinat lokasi berupa longitude latitude, dan lokasi Wi-Fi

15.4. Standar

15.4.1. Organisasi harus mematuhi semua peraturan pelindungan data yang berlaku.

15.4.2. Organisasi harus memiliki prosedur untuk memenuhi hak Subjek Data Pribadi.

15.4.3. Organisasi harus melakukan sosialisasi untuk memastikan semua anggota organisasi memahami urgensi dari pelindungan data pribadi.

15.4.4. Semua karyawan yang menangani atau melakukan pemrosesan Data Pribadi harus menjalankan pelatihan terkait pemrosesan Data Pribadi yang aman.

15.4.5. Insiden terkait keamanan data harus dilaporkan dan ditindaklanjuti sesuai dengan prosedur penanganan insiden dan/atau permohonan Hak Subjek Data Pribadi