KEMENTERIAN PERHUBUNGAN
DIREKTORAT JENDERAL PERHUBUNGAN UDARA

Jl. Medan Merdeka Barat No. 8
Jakarta 10110

Telepon : 3505550 – 3505006 (Sentral)
Fax : 3505136 – 3505139
3507144 – 34833369

Email : djpu151@kemenhub.go.id
Website : hubud.kemenhub.go.id

Nomor : TI.004/793/SDJ.OTL/2026 Jakarta, 14 Agustus 2026
Sifat : **Segera**
Lampiran : 1 (satu) lampiran
Perihal : Imbauan Kehati-hatian dalam Penyajian Informasi pada Media Publik dan Pelindungan Data Pribadi

Yth. Daftar Terlampir

Mendasari Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta dalam rangka meningkatkan keamanan informasi serta mencegah terjadinya penyalahgunaan data dan informasi publik, setiap unit kerja diimbau untuk meningkatkan kehati-hatian dan kewaspadaan dalam publikasi informasi melalui portal, situs web, aplikasi maupun media sosial resmi.

Sehubungan dengan hal tersebut, dimohon kepada seluruh unit kerja untuk memastikan bahwa setiap konten yang dipublikasikan seperti dokumen, foto, video, infografis, tangkapan layar (*screenshot*), maupun bentuk konten lainnya **tidak memuat data pribadi dan/atau informasi sensitif** secara berlebihan atau yang tidak diperlukan untuk kepentingan publikasi.

Adapun data dan informasi yang dilarang dipublikasikan meliputi:

1. Data pribadi, termasuk data pribadi pegawai, yang dapat mengidentifikasi seseorang secara langsung maupun tidak langsung, antara lain:
   a. Nomor Induk Kependudukan (NIK);
   b. Nomor Induk Pegawai (NIP);
   c. tempat dan tanggal lahir;
   d. alamat tempat tinggal;
   e. nomor telepon dan alamat surat elektronik pribadi;
   f. data keluarga dan tanggungan;
   g. nomor rekening dan data keuangan pribadi;
   h. nomor rekening, data keuangan pribadi, dan informasi transaksi keuangan;
   i. dokumen identitas, seperti KTP, Kartu Keluarga, paspor, NPWP, maupun dokumen sejenis;
   j. tanda tangan atau spesimen tanda tangan;
   k. data dan informasi kesehatan;
   l. data biometrik dan genetika;
   m. data anak;
   n. data riwayat kepegawaian yang bersifat rinci dan tidak diperlukan untuk kepentingan publikasi;
   o. kombinasi data lainnya yang dapat digunakan untuk melakukan identifikasi, verifikasi identitas, pemalsuan identitas, maupun rekayasa sosial (*social engineering*).
2. Kredensial akses dan informasi autentikasi sistem, antara lain:
   a. nama pengguna (*username*) dan kata sandi (*password*);
   b. PIN dan *One-Time Password* (OTP);
   c. API *Key*, *secret key*, *access token*, *session token*, dan kredensial elektronik lainnya;
   d. kode QR yang mengandung informasi atau hak akses tertentu; serta
   e. tautan yang memberikan akses langsung terhadap dokumen atau sistem yang bersifat terbatas.

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik
yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).

3. Informasi teknis dan keamanan sistem yang bersifat terbatas, antara lain:
   a. alamat IP internal, konfigurasi jaringan, dan topologi jaringan;
   b. konfigurasi *server*, basis data, sistem, dan aplikasi yang tidak diperuntukkan bagi publik;
   c. dokumentasi teknis yang memuat mekanisme akses internal;
   d. *log* sistem, hasil pengujian keamanan, dan informasi mengenai kerentanan sistem; serta
   e. tangkapan layar aplikasi atau sistem yang memperlihatkan informasi internal, data pribadi, atau informasi akses.
4. Dokumen dan informasi kedinasan yang tidak diperuntukkan bagi publik, termasuk dokumen internal, dokumen terbatas atau rahasia, rancangan dokumen yang belum ditetapkan, serta data dan informasi lainnya yang berdasarkan ketentuan peraturan perundang-undangan atau kebijakan internal dibatasi aksesnya.

Berkenaan dengan hal tersebut, kepada seluruh unit kerja agar:

1. melakukan pemeriksaan dan verifikasi terlebih dahulu terhadap setiap materi sebelum dipublikasikan melalui portal, website, aplikasi, dan/atau media sosial;
2. tidak mempublikasikan daftar atau profil pegawai yang memuat data pribadi dan data kepegawaian secara rinci, kecuali terdapat dasar hukum, kewenangan, dan kebutuhan yang jelas untuk mempublikasikannya;
3. memastikan dokumen seperti surat keputusan, surat tugas, daftar nominatif, daftar hadir, bahan paparan, laporan, formulir, tangkapan layar aplikasi, dan dokumen kepegawaian lainnya telah diperiksa dan tidak menampilkan data pribadi pegawai secara rinci sebelum dipublikasikan;
4. menerapkan prinsip minimalisasi data, yaitu hanya menampilkan data dan informasi yang benar-benar diperlukan sesuai dengan tujuan publikasi;
5. melakukan penyamaran (*masking*), pengaburan (*blurring*), pemotongan (*cropping*), atau penghilangan (*redaction*) terhadap data pribadi dan informasi sensitif yang terdapat dalam dokumen, foto, video, maupun tangkapan layar sebelum dipublikasikan;
6. memastikan dokumen yang akan diunggah telah diperiksa secara menyeluruh, termasuk terhadap lampiran, metadata, kode QR, tanda tangan, tautan, dan informasi lain yang berpotensi mengungkapkan data atau akses yang tidak diperuntukkan bagi publik;
7. melakukan peninjauan kembali terhadap konten yang telah dipublikasikan melalui portal, website, dan media sosial masing-masing unit kerja dan segera melakukan penghapusan, penggantian, penyamaran, atau pembatasan akses apabila ditemukan data pribadi dan/atau informasi sensitif yang tidak seharusnya tersedia secara publik; dan
8. meningkatkan pengawasan terhadap administrator dan pengelola media publik pada masing-masing unit kerja serta memastikan proses publikasi dilaksanakan sesuai dengan ketentuan mengenai pelindungan data pribadi dan keamanan informasi.

Perlu menjadi perhatian bahwa dokumen yang dapat disajikan kepada publik tetap harus melalui pemeriksaan untuk memastikan tidak terdapat bagian yang memuat data pribadi atau informasi sensitif. Apabila diperlukan, bagian tersebut agar disamarkan atau dihilangkan sebelum ditayangkan. Khusus informasi kepegawaian, penyajiannya agar dibatasi pada hal yang relevan dengan kepentingan kedinasan dan pelayanan publik serta tidak memuat rincian yang berpotensi disalahgunakan oleh pihak yang tidak bertanggung jawab. Sejalan dengan hal tersebut, seluruh Aparatur Sipil Negara agar secara konsisten menerapkan ketentuan dalam Surat Edaran Menteri Perhubungan Nomor SE-PHB 2 Tahun 2025 tentang Keamanan Penggunaan Komputer, Perangkat Informasi dan Komunikasi Lainnya, serta Perangkat Lunak oleh Aparatur Sipil Negara di Lingkungan Kementerian Perhubungan, khususnya dalam menjaga keamanan perangkat, akun, kredensial,

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik
yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).

data, dokumen, dan informasi kedinasan serta mencegah akses, penggunaan, penyebarluasan, maupun pengungkapan informasi kepada pihak yang tidak berwenang.

Demikian disampaikan untuk dapat dipedomani dan dilaksanakan. Atas perhatian dan kerja samanya diucapkan terima kasih.

Sekretaris Direktorat Jenderal
Perhubungan Udara,



Achmad Setiyo Prabowo
NIP. 197408191995011001

Tembusan:
Direktur Jenderal Perhubungan Udara

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik
yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).

Lampiran Surat Sesditjen Perhubungan Udara
Nomor : TI.004/793/SDJ.OTL/2026
Tanggal : 14 Agustus 2026

Kepada Yth.:
1. Para Direktur di Lingkungan Direktorat Jenderal Perhubungan Udara;
2. Para Kepala Bagian di Lingkungan Sekretariat Direktorat Jenderal Perhubungan Udara;
3. Para Kepala Kantor Otoritas Bandar Udara Wilayah I – X;
4. Direktur Balai Besar Kalibrasi Fasilitas Penerbangan;
5. Kepala Balai Kesehatan Penerbangan;
6. Kepala Balai Teknik Penerbangan;
7. Para Kepala Kantor Unit Penyelenggara Bandar Udara.

Sekretaris Direktorat Jenderal
Perhubungan Udara,

Achmad Setiyo Prabowo
NIP. 197408191995011001

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik
yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara (BSSN).