KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 3: Perlindungan Data & Etika Digital

Subtopik 3.2: Perlindungan Data Pribadi

Disusun oleh:
Ketut Ananda Dharmawati
NIM: 2215091035

Program Studi S1 Sistem Informasi
Jurusan Teknik Informatika
Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha

BERSAMA CORPU KIWA TENGEN,
KLUNGKUNG TANGGUH HADAPI SERANGAN SIBER

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN KLUNGKUNG
2025

KATA PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat-Nya modul pembelajaran *"Keamanan Siber untuk ASN dan Masyarakat"* dapat disusun hingga membahas subtopik penting mengenai Perlindungan Data Pribadi. Di era digital tahun 2025 ini, data pribadi telah menjadi aset yang sangat berharga sekaligus rentan disalahgunakan. Mulai dari data kependudukan, dokumen resmi, hingga rekam jejak digital, semuanya berpotensi menjadi sasaran kejahatan siber jika tidak dikelola dengan hati-hati.

Subtopik ini disusun untuk memberikan pemahaman kepada ASN dan masyarakat Kabupaten Klungkung tentang pentingnya menjaga keamanan dan kerahasiaan data pribadi. Perlindungan data bukan hanya kewajiban lembaga pemerintah, tetapi juga tanggung jawab individu setiap pengguna layanan digital. Dengan meningkatnya kesadaran dan kedisiplinan dalam mengelola data, kita turut berperan mencegah penyalahgunaan identitas, penipuan digital, serta kebocoran informasi yang dapat merugikan diri sendiri maupun instansi. Terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan subtopik ini. Semoga subtopik ini memberikan manfaat nyata dalam mendukung terwujudnya tata kelola pemerintahan dan kehidupan masyarakat yang lebih aman di era digital.

Kami menyadari bahwa modul ini masih memiliki keterbatasan dan belum sempurna. Oleh karena itu, kami sangat mengharapkan kritik dan saran yang membangun dari para pembaca demi penyempurnaan modul ajar ini di masa mendatang.

Klungkung, 2025

Penyusun

DAFTAR ISI

Tujuan Pembelajaran

Setelah mempelajari bagian ini, peserta (ASN maupun masyarakat) diharapkan mampu:

1. Memahami makna dan jenis data pribadi serta perbedaannya dengan data umum.
2. Mengidentifikasi risiko penyalahgunaan data pribadi seperti pencurian identitas, phishing, atau kebocoran dokumen resmi.
3. Menerapkan langkah-langkah perlindungan data pribadi sesuai prinsip keamanan digital dan UU PDP 2022.
4. Mengetahui prosedur penanganan insiden kebocoran data pribadi melalui saluran resmi pemerintah seperti CSIRT dan aduan.go.id.
5. Menumbuhkan budaya disiplin digital dalam menjaga kerahasiaan data pribadi dan data publik yang dikelola.

Sasaran Peserta

1. ASN: Agar mampu memahami tanggung jawab dalam menjaga kerahasiaan data pribadi warga dan dokumen instansi, mengelola data publik sesuai peraturan UU PDP 2022, serta segera melaporkan apabila terjadi dugaan kebocoran atau penyalahgunaan data pribadi di lingkungan kerja. ASN diharapkan menjadi teladan dalam penerapan tata kelola data yang aman dan etis.
2. Masyarakat: Agar mampu melindungi data pribadi seperti NIK, KK, dan dokumen resmi dari penyalahgunaan, berhati-hati dalam membagikan data ke pihak lain, serta memahami cara melapor ke layanan resmi pemerintah apabila mengalami insiden kebocoran data atau penipuan yang menggunakan identitas pribadi. Dengan kesadaran ini, masyarakat dapat berperan aktif menciptakan lingkungan digital yang aman dan terpercaya.

A. Pengantar: Apa Itu Data Pribadi

Di era layanan digital saat ini, hampir seluruh aktivitas manusia meninggalkan jejak informasi, mulai dari mendaftar layanan publik, berbelanja daring, hingga mengisi formulir online. Semua aktivitas itu menghasilkan **data pribadi**, yaitu informasi yang dapat digunakan untuk mengenali, menghubungi, atau melacak seseorang, baik secara langsung maupun tidak langsung.

Menurut **Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)**, data pribadi didefinisikan sebagai *setiap data tentang individu yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya*. Dengan kata lain, data pribadi adalah bagian dari identitas digital seseorang yang wajib dijaga kerahasiaannya.

1. Jenis Data Pribadi

Secara umum, data pribadi dibagi menjadi dua kategori:

a. Data Pribadi Umum

Merupakan data dasar yang sering digunakan dalam layanan publik. Contohnya:

- ✓ Nama lengkap
- ✓ Nomor Induk Kependudukan (NIK)
- ✓ Nomor Kartu Keluarga (KK)
- ✓ Tempat dan tanggal lahir
- ✓ Alamat dan jenis kelamin

Data ini umumnya digunakan dalam pengurusan administrasi kependudukan, pendidikan, atau pelayanan publik.

b. Data Pribadi Spesifik (Sensitif)

Merupakan data yang sifatnya lebih pribadi dan apabila bocor dapat menimbulkan dampak serius, seperti diskriminasi atau kerugian finansial. Contohnya:

- ✓ Data kesehatan
- ✓ Rekening bank dan transaksi keuangan
- ✓ Citra biometrik (sidik jari, wajah, retina)
- ✓ Agama atau keyakinan
- ✓ Data hukum dan catatan kriminal
- ✓ Dokumen resmi (KTP, ijazah, SK ASN, surat kepemilikan)

2. Mengapa Data Pribadi Penting?

Data pribadi bukan hanya sekadar deretan angka atau teks, **ia mencerminkan identitas seseorang.** Jika bocor atau disalahgunakan, data tersebut dapat digunakan untuk:

a. Mengakses akun atau dokumen resmi seseorang tanpa izin.
b. Melakukan penipuan dengan menggunakan identitas orang lain.
c. Menyebarkan informasi palsu atas nama individu atau instansi.

Oleh sebab itu, menjaga data pribadi berarti **menjaga reputasi, keamanan, dan hak pribadi sebagai warga negara.**

3. Relevansi bagi ASN dan Masyarakat

Bagi **ASN**, data pribadi bukan hanya milik sendiri, tetapi juga milik masyarakat yang dilayani. ASN memiliki tanggung jawab hukum dan moral untuk mengelola data publik secara aman, tidak membagikannya tanpa izin, serta memastikan sistem penyimpanan data instansi terlindungi.

Sedangkan bagi **masyarakat**, kesadaran menjaga data pribadi sangat penting agar tidak mudah tertipu atau menjadi korban kejahatan digital. Mengunggah foto KTP atau dokumen pribadi di media sosial, misalnya, bisa dimanfaatkan pihak tidak bertanggung jawab untuk membuat akun palsu atau pinjaman online.

4. Dasar Hukum Perlindungan Data Pribadi

UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjadi payung hukum utama di Indonesia. Undang-undang ini menegaskan bahwa setiap individu memiliki **hak atas kerahasiaan data pribadi**, dan setiap pihak yang mengelola

data wajib menjaga keamanan serta tidak menyalahgunakannya. **Peraturan Pemerintah No. 71 Tahun 2019** juga mengatur penyelenggaraan sistem elektronik yang aman dan bertanggung jawab.

📘 **Intinya:** Setiap orang, baik ASN maupun masyarakat, harus memahami bahwa data pribadi adalah *aset digital yang tidak bisa sembarangan dibagikan, disimpan, atau dipublikasikan.*

B. Risiko Penyalahgunaan Data Pribadi

Meningkatnya aktivitas digital membuat data pribadi semakin mudah dikumpulkan, disalin, dan disebarluaskan. Banyak kasus kebocoran data di Indonesia terjadi bukan karena peretasan canggih, melainkan karena **kelalaian pengguna atau lemahnya sistem keamanan**. Setiap data pribadi yang tersebar tanpa izin berpotensi dimanfaatkan untuk tindakan kejahatan, penipuan, bahkan pemerasan.

Berikut beberapa risiko yang perlu diwaspadai oleh ASN dan masyarakat:

1. Pencurian Identitas (Identity Theft)

Data seperti NIK, nama lengkap, dan tanggal lahir dapat digunakan oleh pelaku kejahatan untuk **membuat akun palsu, mendaftar pinjaman online, atau mengakses layanan publik** atas nama orang lain. Kasus ini sering terjadi karena pengguna **membagikan foto KTP atau KK** tanpa menyadari risikonya.

🔒 *Ingat: Satu foto KTP bisa digunakan untuk ratusan kejahatan digital.*

2. Phishing dan Penipuan (Scam)

Pelaku kejahatan sering mengaku sebagai petugas instansi, bank, atau penyedia layanan publik. Mereka meminta korban memberikan data seperti NIK, nomor rekening, atau kode OTP. Padahal, **lembaga resmi tidak pernah meminta data pribadi melalui pesan atau telepon.**

Contoh:

“Selamat! Anda mendapat bantuan pemerintah. Silakan kirimkan foto KTP dan KK untuk verifikasi.”

Ini adalah bentuk **phishing** yang bertujuan mencuri data pribadi.

3. Kebocoran Dokumen Resmi

Kasus lain yang sering terjadi adalah **penyebaran dokumen resmi** (KTP, KK, ijazah, SK ASN) di media sosial. Sering kali dilakukan tanpa niat jahat, misalnya untuk menunjukkan keberhasilan atau melengkapi syarat administrasi, tetapi tanpa disadari, informasi pada dokumen itu dapat **digunakan pihak lain untuk penipuan atau pemalsuan data.**

4. Pemalsuan Dokumen dan Manipulasi Data

Data pribadi yang bocor dapat digunakan untuk **memalsukan identitas seseorang**, misalnya membuat surat keterangan kerja, SK palsu, atau dokumen keuangan atas nama korban. Kasus semacam ini tidak hanya merugikan individu, tetapi juga **dapat mencoreng nama baik instansi atau lembaga pemerintah.**

5. Profiling dan Penyalahgunaan Data Digital

Beberapa pihak tidak bertanggung jawab dapat **mengumpulkan data perilaku online** (riwayat pencarian, lokasi, minat) untuk kepentingan bisnis, politik, atau propaganda. Proses ini disebut *profiling digital*, yang dapat mempengaruhi opini publik tanpa sepengetahuan individu.

6. Tren 2025: Kebocoran Data Meningkat

Menurut *Laporan Keamanan Siber Indonesia 2025 (BSSN)*, kasus kebocoran data pribadi di Indonesia meningkat **lebih dari 30% dibanding tahun 2024.** Mayoritas insiden disebabkan oleh:

a. Penggunaan password lemah
b. Kurangnya verifikasi dua langkah (2FA)
c. Pengunggahan dokumen pribadi di media sosial
d. Kecerobohan dalam membagikan data ke situs tidak resmi

7. Dampak Nyata bagi ASN dan Masyarakat

Bagi ASN: dapat menurunkan kepercayaan publik, memicu kebocoran data instansi, dan berpotensi sanksi disiplin.

Bagi masyarakat: dapat kehilangan uang, identitas disalahgunakan, dan reputasi pribadi tercemar.

C. Prinsip Perlindungan Data Pribadi

Perlindungan data pribadi tidak hanya soal teknologi, tetapi juga soal **tanggung jawab dan etika dalam mengelola informasi seseorang.** Baik ASN maupun masyarakat wajib memahami prinsip dasarnya agar tidak melanggar hukum atau menimbulkan kerugian bagi pihak lain. Berikut **7 prinsip utama perlindungan data pribadi** yang harus diterapkan dalam setiap aktivitas digital:

1. Keterbukaan (Transparency)

Pemilik data berhak mengetahui **tujuan dan cara penggunaan datanya.** Instansi atau pihak yang meminta data wajib menjelaskan **mengapa data dikumpulkan, untuk apa digunakan, dan siapa yang akan mengelolanya.**

Contoh: Saat ASN mengumpulkan data warga untuk layanan publik, wajib ada pemberitahuan tertulis atau digital mengenai tujuan pengumpulan data.

2. Persetujuan yang Jelas (Explicit Consent)

Setiap pengumpulan atau pemrosesan data harus dilakukan **dengan izin eksplisit dari pemilik data.** Tanpa persetujuan, tindakan itu dapat dianggap pelanggaran hukum.

Contoh: Aplikasi layanan publik harus memiliki fitur “setuju” atau “izin penggunaan data” sebelum mengakses NIK atau dokumen pengguna.

3. Pembatasan Tujuan (Purpose Limitation)

Data hanya boleh digunakan **sesuai dengan tujuan awal pengumpulan.** Jika data dikumpulkan untuk keperluan administrasi, maka tidak boleh dipakai untuk promosi, survei, atau kegiatan lain tanpa izin tambahan.

Contoh: Data pendaftaran vaksin tidak boleh digunakan untuk iklan produk kesehatan.

4. Keamanan & Kerahasiaan (Security & Confidentiality)

Setiap data pribadi harus dilindungi dari **akses, penggunaan, atau pengungkapan yang tidak sah.** ASN dan instansi harus menerapkan **sistem keamanan**

berlapis, seperti enkripsi, pembatasan akses, dan audit berkala. ASN dilarang menyimpan data warga di perangkat pribadi tanpa izin pimpinan atau tanpa perlindungan kata sandi.

5. Akses Terbatas (Limited Access)

Tidak semua orang di instansi boleh melihat atau mengelola data pribadi. Akses hanya diberikan kepada pihak yang memang membutuhkan untuk menjalankan tugasnya.

Contoh: Petugas administrasi kependudukan boleh mengakses data NIK, tetapi tidak boleh menyebarkannya ke luar sistem.

6. Ketepatan & Pembaruan Data (Accuracy)

Data yang disimpan harus **akurat, mutakhir, dan sesuai fakta.** Pemilik data juga berhak meminta pembaruan jika terdapat kesalahan.

Contoh: Masyarakat bisa meminta pembetulan data KK atau KTP jika terjadi kesalahan penulisan nama.

7. Hak Individu atas Data (Individual Rights)

Setiap orang memiliki hak untuk:

a. **Melihat** data pribadinya yang tersimpan.
b. **Memperbaiki atau menghapus** data yang tidak relevan.
c. **Menolak** pemrosesan data untuk tujuan tertentu.

Hak ini diatur dalam **Pasal 4 sampai Pasal 9 UU PDP**, dan harus dihormati oleh instansi pemerintah maupun swasta.

⚖️ Penerapan dalam Konteks ASN dan Masyarakat

Bagi ASN: Harus memahami bahwa setiap data warga bukan hanya angka administratif, tetapi **identitas hukum yang dilindungi undang-undang.** Pelanggaran terhadap prinsip ini dapat berakibat **sanksi administratif, pidana, dan etik.**

Bagi Masyarakat: Wajib berhati-hati saat memberikan data pribadi. Pastikan pihak penerima data memiliki **izin resmi** dan jelas tujuannya. Masyarakat juga berhak **menolak** jika merasa datanya diminta tanpa alasan yang sah.

📘 **Contoh Penerapan Nyata (Klungkung, 2025):**

Pemerintah Kabupaten Klungkung menerapkan sistem **e-Government** yang mewajibkan setiap aplikasi SPBE (Sistem Pemerintahan Berbasis Elektronik) memiliki **kebijakan privasi dan enkripsi data pengguna**. Kebijakan ini merupakan bagian dari penerapan prinsip *keterbukaan, keamanan, dan hak individu.*

D. Cara Melindungi Data Pribadi Sehari-hari

Melindungi data pribadi tidak harus rumit. Banyak kebocoran data terjadi bukan karena peretasan, tapi karena **kebiasaan digital yang ceroboh.** ASN dan masyarakat perlu membangun disiplin sederhana dalam kehidupan digital sehari-hari untuk menjaga keamanan informasi pribadi.

Berikut langkah-langkah praktis yang bisa diterapkan:

1. Hindari Mengunggah Dokumen Pribadi di Media Sosial

Jangan pernah memposting **foto KTP, KK, kartu vaksin, boarding pass, ijazah, atau SK ASN** di platform publik. Data pada dokumen tersebut dapat digunakan oleh orang lain untuk **membuat identitas palsu, mengajukan pinjaman, atau penipuan online.**

✅ **Contoh baik:** Tutupi sebagian informasi penting (NIK, alamat, tanda tangan) jika harus membagikan dokumen untuk verifikasi.

2. Gunakan Password yang Kuat dan Berbeda untuk Setiap Akun

Password adalah kunci utama data pribadi Anda. Gunakan kombinasi **huruf besar, kecil, angka, dan simbol** (minimal 12 karakter). Hindari password mudah ditebak seperti *tanggal lahir, nama anak, atau 123456.*

💡 **Tips:** Gunakan *password manager* agar tidak perlu menghafal semua kata sandi secara manual.

3. Aktifkan Verifikasi Dua Langkah (Two-Factor Authentication / 2FA)

Tambahkan lapisan keamanan ekstra dengan mengaktifkan 2FA di akun penting seperti **email, e-office, e-formasi, atau perbankan digital.** Dengan 2FA, meskipun

password bocor, pelaku tidak dapat masuk tanpa kode verifikasi tambahan.

4. Simpan Dokumen di Tempat Aman

Simpan file penting (KTP, KK, SK ASN, ijazah) hanya di perangkat pribadi atau **folder terenkripsi.** Gunakan **flashdisk pribadi** atau layanan penyimpanan cloud yang memiliki keamanan tinggi (*encrypted cloud*).

Hindari menyimpan dokumen di komputer umum, warnet, atau grup WhatsApp kerja.

5. Pastikan Keaslian Situs atau Aplikasi

Sebelum memasukkan data pribadi secara online, **periksa alamat situs (URL).** Pastikan situs diawali dengan https:// dan berasal dari domain resmi seperti **.go.id, .org, atau .ac.id.**

❌ Contoh palsu: dukcapil-verify-id.com

✅ Contoh resmi: dukcapil.kemendagri.go.id

6. Waspadai Permintaan Data Pribadi

Jika ada pihak yang meminta data melalui pesan, panggilan, atau email — **jangan langsung percaya.** Instansi resmi tidak akan meminta data pribadi tanpa surat resmi atau saluran komunikasi resmi.

🚫 Jangan kirimkan foto KTP, nomor rekening, atau OTP melalui chat pribadi.

✅ Laporkan jika ada pihak yang mencurigakan ke kanal aduan pemerintah.

7. Gunakan Aplikasi dan Layanan Resmi Pemerintah

Untuk urusan administrasi seperti e-KTP, Dukcapil, atau layanan ASN, **gunakan hanya aplikasi resmi.** Hindari situs atau aplikasi pihak ketiga yang mengaku dapat membantu mempercepat proses — banyak di antaranya **mengumpulkan data tanpa izin.**

Contoh aman: *https://layanan.dukcapil.kemendagri.go.id/*

8. Laporkan Jika Terjadi Kebocoran Data

Apabila Anda menemukan data pribadi tersebar, segera laporkan ke:

a. **CSIRT daerah** (jika ASN)

b. **Otoritas Pelindungan Data Pribadi (OPDP)**, lembaga pengawas yang akan aktif penuh pada 2025

Pelaporan cepat membantu mencegah penyalahgunaan data lebih lanjut.

9. Edukasi Keluarga dan Rekan Kerja

Lindungi data tidak cukup hanya untuk diri sendiri. Edukasi keluarga, rekan kerja, dan lingkungan sekitar tentang **bahaya membagikan data sembarangan.** Kebiasaan digital yang baik akan menciptakan **ekosistem masyarakat digital yang lebih aman.**

E. Regulasi & Dasar Hukum Perlindungan Data Pribadi

Perlindungan data pribadi di Indonesia memiliki dasar hukum yang kuat. Negara mengatur hak dan kewajiban semua pihak, baik pemerintah, swasta, maupun masyarakat dalam menjaga kerahasiaan dan keamanan data pribadi. Tujuan utamanya adalah **melindungi identitas warga, mencegah penyalahgunaan data, serta memastikan kepercayaan terhadap layanan digital pemerintah.**

Berikut regulasi dan dasar hukum utama yang berlaku hingga tahun 2025:

1. Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)

Merupakan **aturan utama** yang mengatur bagaimana data pribadi dikumpulkan, digunakan, disimpan, dan dibagikan. UU ini menegaskan bahwa **data pribadi adalah hak asasi manusia.**

Beberapa poin penting:

a. Wajib ada **persetujuan jelas** dari pemilik data.
b. Pemilik data berhak **mengakses, memperbaiki, dan menghapus** datanya.
c. Pelanggaran terhadap data pribadi dapat dikenakan **sanksi administratif dan pidana.**
d. Dibentuk **Otoritas Pelindungan Data Pribadi (OPDP)** sebagai lembaga pengawas independen.

📌 UU PDP berlaku penuh mulai tahun 2024, dan pada 2025 semua instansi wajib

menyesuaikan sistemnya dengan ketentuan ini.

2. Peraturan Pemerintah (PP) No. 71 Tahun 2019

Tentang **Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).** PP ini mengatur tanggung jawab penyelenggara sistem elektronik, termasuk instansi pemerintah dan pelaku usaha digital.

Poin penting:

a. Penyelenggara sistem wajib menjaga **kerahasiaan dan integritas data pribadi pengguna.**
b. Harus menyediakan **mekanisme penghapusan data** bila diminta oleh pemilik data.
c. Wajib melaporkan **insiden kebocoran data** kepada pemerintah.

3. Peraturan Menteri Kominfo No. 20 Tahun 2016

Tentang **Perlindungan Data Pribadi dalam Sistem Elektronik.** Menjadi pedoman teknis bagi lembaga dan penyedia layanan digital dalam mengelola data pribadi.

Beberapa ketentuan:

a. Harus ada **notifikasi kepada pemilik data** jika terjadi kebocoran.
b. Data pribadi tidak boleh **dipindahkan ke luar negeri** tanpa izin.
c. Wajib melakukan **audit keamanan sistem secara berkala.**

4. Peraturan Badan Siber dan Sandi Negara (BSSN)

BSSN mengeluarkan berbagai panduan teknis terkait **keamanan siber, manajemen insiden, dan perlindungan data.** ASN dan instansi wajib mengikuti standar keamanan yang ditetapkan, termasuk:

a. *Pedoman Teknis Keamanan Data Elektronik (2024)*
b. *Standar Prosedur Penanganan Insiden Siber (CSIRT)*
c. BSSN juga membina **CSIRT (Computer Security Incident Response Team)** di tingkat daerah, termasuk **CSIRT Kabupaten Klungkung**, untuk menindaklanjuti insiden kebocoran data.

5. Otoritas Pelindungan Data Pribadi (OPDP)

Mulai beroperasi penuh pada tahun **2025** sebagai lembaga pengawas independen di bawah Kementerian Kominfo.

Tugas OPDP:

a. Mengawasi pelaksanaan UU PDP.
b. Menerima laporan pelanggaran atau kebocoran data.
c. Memberikan sanksi administratif bagi pelanggar.
d. Melakukan sosialisasi dan edukasi publik tentang perlindungan data.

💡 ASN dan masyarakat dapat mengajukan laporan ke OPDP jika menemukan indikasi penyalahgunaan data pribadi oleh pihak tertentu.

6. Kewajiban ASN dan Pemerintah Daerah

Bagi ASN, regulasi ini menjadi dasar untuk:

a. Menjamin keamanan data masyarakat dalam sistem SPBE.
b. Tidak menyebarkan data pribadi tanpa izin.
c. Melakukan pelaporan insiden ke CSIRT atau Kominfo jika terjadi kebocoran.

Pemerintah daerah juga diwajibkan **membangun kebijakan perlindungan data daerah**, termasuk:

a. Menunjuk pejabat khusus bidang keamanan data.
b. Menyusun SOP perlindungan data pribadi.
c. Mengedukasi pegawai dan masyarakat lokal.

📘 **Rangkuman Singkat Regulasi:**

No	Regulasi	Pokok Pengaturan	Tahun Berlaku
1	UU No. 27/2022	Hak & kewajiban pelindungan data pribadi	2022 (efektif 2024)
2	PP No. 71/2019	Penyelenggaraan sistem & transaksi elektronik	2019

3	Permenkominfo No. 20/2016	Tata kelola data pribadi di sistem elektronik	2016
4	Peraturan BSSN	Standar keamanan siber & penanganan insiden	2024
5	OPDP (Otoritas PDP)	Pengawasan dan penegakan hukum data pribadi	2025

F. Peran ASN dan Masyarakat

Perlindungan data pribadi tidak hanya menjadi urusan lembaga pusat atau ahli teknologi, tetapi juga **tanggung jawab bersama seluruh elemen bangsa.** ASN dan masyarakat sama-sama berperan penting dalam membangun budaya digital yang aman, etis, dan bertanggung jawab.

Berikut peran dan langkah nyata yang perlu dilakukan oleh masing-masing pihak 👇

1. Peran Aparatur Sipil Negara (ASN)

ASN adalah **garda depan dalam menjaga kepercayaan publik terhadap layanan digital pemerintah.** Mereka mengelola banyak data sensitif, seperti data kependudukan, keuangan, dan administrasi publik, sehingga harus menjaga kerahasiaannya dengan disiplin.

Peran utama ASN meliputi:

a. Menjamin Keamanan Data Warga

ASN wajib memastikan seluruh data yang dikelola instansinya disimpan dalam sistem yang **aman, terenkripsi, dan terkontrol aksesnya.** Misal: Tidak menyimpan file berisi NIK atau KK warga di komputer pribadi tanpa izin pimpinan.

b. Tidak Membagikan Dokumen Publik Tanpa Izin

Semua bentuk penyebaran data, baik melalui email, grup WhatsApp, maupun media sosial, harus mendapatkan **persetujuan resmi** dari atasan atau

pejabat berwenang. ASN yang lalai dapat dikenakan sanksi etik dan administratif sesuai UU ASN dan UU PDP.

c. Menggunakan Email dan Platform Resmi Pemerintah

ASN wajib menggunakan **akun dan sistem berakhiran .go.id** untuk komunikasi dan pertukaran data dinas. Hal ini bertujuan agar data terekam, terlindungi, dan tidak bocor melalui platform komersial.

d. Menjadi Teladan Keamanan Digital

Sebagai pelayan publik, ASN harus menjadi contoh bagi masyarakat dalam menggunakan teknologi dengan aman. Contoh: Tidak membagikan foto dokumen kerja di media sosial, menggunakan password kuat, dan aktif dalam pelatihan keamanan siber.

e. Melaporkan Insiden Kebocoran Data

Jika mengetahui adanya kebocoran data, ASN harus **segera melaporkannya ke unit keamanan (CSIRT) instansi** untuk dilakukan penanganan sesuai prosedur. Keterlambatan laporan dapat memperbesar dampak dan merugikan publik.

2. Peran Masyarakat

Masyarakat adalah **pemilik sah data pribadi**, sehingga mereka memiliki hak sekaligus tanggung jawab untuk menjaganya. Perlindungan data dimulai dari kesadaran setiap individu saat beraktivitas di dunia digital. Peran masyarakat meliputi:

a. Berhati-hati Saat Berbagi Data

Tidak semua pihak yang meminta data adalah lembaga resmi. Selalu **verifikasi keaslian situs atau petugas** sebelum mengisi formulir atau memberikan informasi pribadi.

💡 *Jangan pernah membagikan foto KTP, KK, atau nomor rekening di media sosial, meski untuk keperluan undian atau promo.*

b. Menggunakan Layanan Resmi Pemerintah

Untuk pengurusan dokumen seperti KTP, KK, atau akta, gunakan hanya

platform resmi pemerintah, seperti:

https://layanan.dukcapil.kemendagri.go.id/

https://kominfo.go.id/

Hindari aplikasi pihak ketiga yang tidak jelas asal-usulnya.

c. Melapor Jika Terjadi Kebocoran Data

Masyarakat berhak melapor jika merasa datanya disalahgunakan atau bocor.

Laporan dapat dikirim ke:

CSIRT Klungkung untuk kejadian di tingkat daerah

Otoritas Pelindungan Data Pribadi (OPDP) (aktif penuh 2025)

d. Mendidik Keluarga dan Lingkungan

Kesadaran keamanan digital harus dimulai dari rumah. Orang tua dapat memberi contoh kepada anak-anak untuk **tidak sembarangan membagikan foto, dokumen, atau lokasi pribadi.**

⚠️ **Peringatan Penting**

ASN maupun masyarakat dapat **dikenai sanksi hukum** apabila:

a. Menyebarkan data pribadi tanpa izin.
b. Menggunakan data orang lain untuk kepentingan pribadi atau politik.
c. Tidak melaporkan kebocoran data yang diketahuinya.

UU PDP (Pasal 67–69) menetapkan sanksi administratif, denda, dan pidana bagi pelanggar, tergantung tingkat kesalahannya.

G. Alur Penanganan Insiden Data Pribadi

Kebocoran data pribadi bisa terjadi kapan saja, baik karena kesalahan teknis, kelalaian pengguna, maupun serangan siber. Yang paling penting bukan hanya **mencegah**, tetapi juga **menangani dengan benar** ketika insiden terjadi. Prosedur penanganan insiden harus dilakukan secara cepat, terkoordinasi, dan sesuai dengan standar nasional keamanan siber yang diatur oleh **Badan Siber dan Sandi Negara (BSSN)**

serta **UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).**

1. Deteksi Awal (Identifikasi Insiden)

Langkah pertama adalah **mengenali gejala adanya kebocoran data.** Indikator awal bisa berupa:

a. Munculnya laporan masyarakat tentang penyalahgunaan data.
b. File dokumen (seperti KK, NIK, atau SK) tersebar di media sosial.
c. Sistem instansi menunjukkan aktivitas login mencurigakan.
d. Ada permintaan data tidak biasa dari pihak luar.

💡 *Deteksi dini sangat penting. Semakin cepat diketahui, semakin kecil risiko dampaknya terhadap publik.*

2. Verifikasi dan Pengamanan Sementara

Setelah dugaan kebocoran muncul, tim teknis instansi harus segera:

a. **Memverifikasi kebenaran laporan** (apakah benar terjadi kebocoran).
b. **Menutup akses sementara** ke sistem atau database yang terdampak.
c. **Membuat salinan forensik (backup)** untuk investigasi.
d. **Melindungi bukti digital** agar tidak dihapus atau diubah.

Tujuannya agar sumber masalah bisa ditemukan tanpa memperparah kerusakan data.

3. Pelaporan ke Unit Keamanan (CSIRT)

Setiap instansi pemerintah wajib memiliki atau berkoordinasi dengan **CSIRT (Computer Security Incident Response Team)**, tim resmi pemerintah yang menangani insiden siber.

Langkah pelaporan:

a. ASN yang menemukan insiden melapor ke atasan langsung atau petugas keamanan data instansi.
b. Laporan diteruskan ke **CSIRT instansi** (atau **CSIRT Kabupaten Klungkung** untuk lingkup daerah).
c. Jika berdampak luas, laporan diteruskan ke **BSSN** dan **Kementerian Kominfo.**

4. Koordinasi dengan Pihak Terkait

Jika insiden berdampak besar (misalnya data kependudukan, keuangan, atau dokumen ASN bocor), maka instansi wajib:

a. **Melapor ke Otoritas Pelindungan Data Pribadi (OPDP)**, lembaga nasional pengawas perlindungan data (aktif penuh pada 2025).
b. **Berkoordinasi dengan Kominfo** untuk penghapusan data yang tersebar di platform publik.
c. **Melibatkan BSSN** untuk analisis forensik dan rekomendasi teknis.

🔒 Transparansi dan koordinasi adalah kunci. Jangan menutupi insiden karena akan memperburuk dampaknya.

5. Pemberitahuan kepada Pemilik Data (Masyarakat)

UU PDP mewajibkan pengendali data (misal: instansi pemerintah) untuk **memberi tahu masyarakat yang datanya bocor** dalam waktu maksimal **3 x 24 jam** sejak insiden diketahui.

Pemberitahuan harus mencakup:

a. Jenis data yang terdampak
b. Tindakan yang sudah dilakukan
c. Langkah yang disarankan kepada pemilik data (misalnya mengganti password, memblokir rekening, dsb.)

Contoh: Jika data NIK dan KK bocor, warga diminta memeriksa penggunaan data tersebut di aplikasi resmi pemerintah seperti *cekdptonline.kpu.go.id* atau *layanan.dukcapil.kemendagri.go.id.*

6. Pemulihan Sistem dan Evaluasi Keamanan

Setelah insiden dikendalikan, instansi harus segera:

a. Memperbaiki celah keamanan (patching, update sistem, atau audit ulang akses).
b. Melatih kembali pegawai terkait keamanan data dan etika digital.
c. Melakukan evaluasi kebijakan internal agar kejadian tidak terulang.

Hasil evaluasi biasanya dituangkan dalam laporan pasca-insiden (post-incident report)

dan menjadi bahan pembelajaran nasional.

7. Dokumentasi dan Pelaporan Akhir

Semua proses penanganan, mulai dari deteksi, laporan, hingga pemulihan, wajib **didokumentasikan secara resmi.**

Dokumen ini penting untuk:

a. Bukti kepatuhan terhadap UU PDP
b. Referensi untuk audit keamanan berikutnya
c. Dasar penyusunan SOP baru di instansi

🧩 Peran CSIRT (Computer Security Incident Response Team)

CSIRT merupakan **tim resmi pemerintah** yang bertugas menangani dan memulihkan insiden siber, termasuk kebocoran data. CSIRT Klungkung dibentuk untuk membantu instansi daerah dan masyarakat menangani insiden secara cepat dan terkoordinasi.

Tugas utama CSIRT Klungkung:

a. Menerima laporan insiden siber dari ASN dan masyarakat.
b. Melakukan investigasi dan analisis penyebab insiden.
c. Memberikan rekomendasi pemulihan keamanan sistem.
d. Melakukan koordinasi dengan BSSN dan Kominfo bila insiden berdampak luas.

📞 **Kontak CSIRT Klungkung (contoh format, disesuaikan dengan instansi):**

Situs resmi: *https://csirtklungkung.klungkungkab.go.id/*

H. Rekomendasi untuk ASN dan Masyakarat

👨‍💼 Untuk ASN:

1. Terapkan prinsip **“least privilege”** hanya mengakses data yang memang diperlukan untuk tugas.
2. Gunakan **akun resmi pemerintah (.go.id)** untuk komunikasi terkait data publik.
3. Ikuti pelatihan keamanan data dan siber minimal **dua kali setahun**.

4. Segera laporkan insiden kebocoran data kepada **CSIRT Klungkung**.
5. Pastikan dokumen warga disimpan di sistem aman dengan **enkripsi dan otorisasi berlapis**.

👥 Untuk Masyarakat:

1. Hindari mengunggah dokumen pribadi (KTP, KK, SIM, paspor) di media sosial atau grup chat.
2. Gunakan layanan resmi pemerintah seperti **Dukcapil Online** atau **SPBE daerah** untuk pengurusan dokumen.
3. Aktifkan **verifikasi dua langkah (2FA)** di akun penting seperti email, media sosial, dan e-wallet.
4. Segera lapor ke **aduan.go.id** jika data pribadi disalahgunakan.
5. Edukasi keluarga dan komunitas sekitar tentang pentingnya menjaga data pribadi.

I. Arah Penguatan ke Depan (2025 dan seterusnya)

Tahun 2025 menjadi tonggak penting bagi keamanan data di Indonesia, dengan mulai beroperasinya **Otoritas Pelindungan Data Pribadi (OPDP)**. Kabupaten Klungkung dapat memanfaatkan momentum ini untuk:

1. Menguatkan **kebijakan SPBE daerah** berbasis perlindungan data.
2. Mengintegrasikan layanan aduan insiden data pribadi ke **CSIRT Klungkung.**
3. Menyelenggarakan **program literasi digital tahunan** bagi ASN dan masyarakat umum.
4. Membangun budaya digital yang aman, transparan, dan beretika di setiap lapisan masyarakat.

Perlindungan data pribadi adalah fondasi dari **kepercayaan digital**. Tanpa keamanan dan kesadaran, layanan digital pemerintah akan kehilangan kredibilitas. Melalui pemahaman bersama antara ASN dan masyarakat, Klungkung dapat menjadi contoh daerah dengan **ekosistem digital yang tangguh, aman, dan beretika.**

“Melindungi data pribadi berarti melindungi identitas, martabat, dan masa depan kita di dunia digital.”

Pertanyaan Reflektif

1. Pernahkah Anda membagikan data pribadi (misalnya NIK, KK, foto KTP) di media sosial atau aplikasi tanpa memikirkan risikonya? Apa yang Anda rasakan setelah memahami dampaknya?
2. Mengapa Anda perlu tahu tujuan dan pihak yang meminta data pribadi sebelum memberikannya?
3. Sebagai ASN, bagaimana Anda memastikan data masyarakat yang dikelola tidak tersebar ke pihak lain tanpa izin? Jika Anda masyarakat, bagaimana Anda melindungi data keluarga dari penipuan digital?
4. Dalam pandangan Anda, apakah membocorkan data pribadi orang lain, meski tanpa niat jahat, bisa dianggap pelanggaran etika digital? Jelaskan alasannya.
5. Bagaimana Anda menanggapi teman atau rekan kerja yang membagikan dokumen resmi di grup chat tanpa menyadari risikonya?

DAFTAR PUSTAKA

Badan Pusat Statistik (BPS). (2025). *Statistik Penggunaan Internet dan Keamanan Digital Indonesia 2025.* Jakarta: BPS RI.

Badan Siber dan Sandi Negara (BSSN). (2025). *Laporan Keamanan Siber Nasional 2025.* Jakarta: BSSN RI.

Cybersecurity Indonesia. (2025). *Tren Keamanan Siber dan Perlindungan Data Pribadi di Indonesia 2025.* Jakarta: Pusat Kajian Keamanan Digital.

European Union. (2018). *General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679.* Official Journal of the European Union.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). *Pedoman Perlindungan Data Pribadi dalam Sistem Elektronik.* Jakarta: Direktorat Jenderal Aplikasi Informatika.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2016). *Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.* Jakarta: Kominfo.

Organisation for Economic Co-operation and Development (OECD). (2023). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Paris: OECD Publishing.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.* Lembaran Negara Republik Indonesia Tahun 2022 Nomor 181.

Republik Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE).* Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185.

UNESCO. (2024). *Ethical Guidelines for Digital Transformation and Data Privacy in Public Administration.* Paris: UNESCO Publishing.