Panduan Lengkap Kepatuhan UU PDP untuk Website Bisnis Indonesia

Undang-Undang Pelindungan Data Pribadi — Apa yang Harus Dipenuhi Website Bisnis Kamu

Buatan ShortcutSistem · shortcutsistem.com

Pendahuluan: Kenapa UU PDP Penting untuk Website

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) adalah regulasi besar di Indonesia yang mengatur bagaimana bisnis mengumpulkan, menyimpan, dan menggunakan data pribadi pengguna. UU ini sudah berlaku dan mengatur semua entitas yang memproses data pribadi penduduk Indonesia — termasuk website bisnis.

Apa artinya ini untuk pemilik website? Jika website kamu mengumpulkan data pribadi pengunjung — melalui formulir kontak, akun pengguna, cookies, newsletter, atau checkout — maka website kamu Wajib memenuhi persyaratan UU PDP. Ketidakpatuhan bisa berujung pada denda hingga 5% dari pendapatan tahunan atau penjara bagi individu yang bertanggung jawab.

 Panduan ini membantu kamu memahami 10 persyaratan utama UU PDP yang berkaitan langsung dengan website bisnis, beserta checklist untuk memastikan website kamu comply. Gunakan Security Audit dari ShortcutSistem untuk memeriksa kepatuhan website kamu secara otomatis.

10 Persyaratan UU PDP untuk Website

Berikut 10 area yang harus dipenuhi website bisnis kamu berdasarkan UU PDP. Setiap section disertai explanation, contoh, dan checklist.

1. Transparency — Informasi Pengumpulan Data

Persyaratan: Pengguna harus tahu secara jelas sebelum memberikan data: (a) siapa yang mengumpulkan data, (b) jenis data apa yang dikumpulkan, (c) tujuan pengumpulan, (d) berapa lama data disimpan, dan (e) bagaimana data dilindungi.

Contoh di website:

- Halaman Privacy Policy yang menjelaskan semua hal di atas
- Popup atau banner cookie consent saat pertama kali kunjungan
- Checkbox persetujuan ('I agree to the Privacy Policy') di formulir
- Notifikasi saat ada perubahan Privacy Policy

 Contoh teks yang baik: 'Kami mengumpulkan nama dan email kamu untuk keperluan newsletter. Data disimpan selama 2 tahun dan tidak dibagikan ke pihak ketiga. Hubungi kami untuk mengakses atau menghapus data kamu.'

 Checklist: Apakah Privacy Policy kamu menyebutkan siapa, apa, kenapa, berapa lama, dan bagaimana data dilindungi?

2. Lawful Basis — Dasar Hukum Pengumpulan Data

Persyaratan: Setiap pengumpulan data pribadi harus memiliki dasar hukum yang jelas. UU PDP mengatur 6 dasar hukum: persetujuan (consent), выполнение договора (kontrak), pflicht nach Gesetz (kewajiban hukum), kepentingan vital, tugas berdasarkan pelayanan umum, dan kepentingan sah (legitimate interest).

- Jika menggunakan formulir kontak: persetujuan explisit diperlukan
- Jika memproses transaksi: dasar hukum adalah выполнение договора (kontrak)
- Jika cookie analitik: persetujuan diperlukan di Indonesia

 Checklist: Apakah kamu bisa menjelaskan dasar hukum untuk setiap jenis data yang kamu kumpulkan?

3. Consent Management — Pengelolaan Persetujuan

Persyaratan: Persetujuan harus diberikan secara eksplisit, spesifik, dan berdasarkan informasi yang jelas. Tidak boleh menggunakan consent yang tersembunyi, checkbox yang sudah terisi, atau persetujuan yang digabungkan dengan syarat lain.

- Checkbox terpisah untuk setiap tujuan: newsletter, analitik, marketing
- Tombol 'Terima' atau 'Setuju' yang jelas (bukan 'X' untuk menolak)
- Pilihan untuk menarik persetujuan kapan saja

 Contoh implementasi yang baik: Banner cookie dengan tombol 'Terima Semua', 'Tolak', dan 'Pengaturan Cookie' yang membuka panel pilihan.

 Checklist: Apakah formulir dan cookie banner kamu menggunakan consent eksplisit?

4. Data Subject Rights — Hak Subjek Data

Persyaratan: Pengguna memiliki hak untuk: (1) Mendapatkan salinan data mereka, (2) Memperbaiki data yang tidak akurat, (3) Menghapus data mereka, (4) Membatasi pemrosesan, (5) Menarik persetujuan, (6) Mengajukan keberatan. Bisnis wajib merespons dalam waktu 3x24 jam.

- Halaman Privacy Policy harus menyebutkan bagaimana cara menggunakan hak-hak ini
- Alamat email atau formulir khusus untuk mengajukan permintaan hak subjek data
- Proses internal untuk merespons permintaan dalam 3x24 jam

 Tambahkan di Privacy Policy: 'Untuk mengakses, memperbaiki, atau menghapus data pribadi kamu, hubungi kami di [email] atau via WhatsApp [nomor]. Kami akan merespons dalam 3x24 jam.'

 Checklist: Apakah website kamu menyediakan cara jelas bagi pengguna untuk menggunakan hak-hak mereka?

5. Data Protection Officer (DPO) — Pejabat Pelindungan Data

Persyaratan: Jika bisnis memproses data dalam volume besar atau sensitif, diwajibkan menunjuk DPO. Untuk bisnis kecil, masih direkomendasikan meskipun tidak wajib.

- DPO harus bisa dihubungi: nama, email, dan/atau nomor telepon
- DPO tidak boleh merangkap sebagai pengambil keputusan utama dalam pemrosesan data yang sama
- Jika volume kecil: wajib menyebutkan contact person yang bertanggung jawab untuk privasi

 Untuk UMKM: cukup cantumkan 'Untuk pertanyaan terkait data pribadi, hubungi [Nama] di [email/nomor WA]' di Privacy Policy.

 Checklist: Apakah Privacy Policy kamu menyebutkan kontak untuk pertanyaan data pribadi?

6. Data Security — Keamanan Data

Persyaratan: Bisnis wajib menerapkan langkah-langkah keamanan yang tepat untuk melindungi data pribadi. Tingkat keamanan harus sesuai dengan risiko pemrosesan data.

- Enkripsi data saat transit (HTTPS/TLS) dan saat istirahat (enkripsi storage)
- Akses terbatas: hanya orang yang berkepentingan yang bisa mengakses data
- Autentikasi dua faktor (2FA) untuk admin dashboard
- Pencadangan data (backup) secara berkala
- Monitoring keamanan dan respons insiden

 Gunakan Security Audit dari ShortcutSistem untuk mengecek apakah website kamu sudah menerapkan security headers yang benar (CSP, HSTS, X-Frame-Options).

 Checklist: Apakah website kamu sudah menggunakan HTTPS? Apakah admin dashboard dilindungi dengan password kuat dan 2FA?

7. Cookie Consent — Persetujuan Cookie

Persyaratan: Di Indonesia, penggunaan cookies yang mengumpulkan data pribadi memerlukan persetujuan explisit dari pengguna. Banner cookie harus memberikan opsi untuk menerima atau menolak setiap kategori cookie.

- Kategori cookie yang harus disebutkan: Essential (wajib), Analytics, Functional, Marketing
- Opsi untuk menolak cookie non-esensial
- Tidak menggunakan cookie sebelum persetujuan diberikan (kecuali essential)
- Informasi jelas tentang siapa yang mengelola cookie (first-party vs third-party)

 Contoh teks banner: 'Kami menggunakan cookies untuk meningkatkan pengalaman browsing kamu. Cookies esensial wajib aktif. Cookies analitik dan marketing memerlukan persetujuan. [Terima Semua] [Tolak] [Pengaturan]'

 Checklist: Apakah website kamu memiliki cookie banner dengan opsi penolakan yang jelas?

8. Third-Party Data Sharing — Pembagian Data ke Pihak Ketiga

Persyaratan: Jika bisnis membagikan data ke pihak ketiga (vendor, partner, Google Analytics, payment gateway), wajib ada perjanjian kerahasiaan (NDA/PPA) dan transparency tentang hal ini.

- Privacy Policy harus menyebutkan pihak ketiga yang menerima data
- Pastikan vendor pihak ketiga juga comply dengan UU PDP
- Contoh: Google Analytics, Meta Pixel, payment gateway (Midtrans), email service (Mailchimp)

 Tambahkan di Privacy Policy: 'Kami berbagi data dengan [nama vendor] untuk [tujuan]. Vendor ini terikat perjanjian kerahasiaan dan hanya menggunakan data untuk keperluan yang kami tentukan.'

 Checklist: Apakah Privacy Policy kamu menyebutkan semua vendor/pihak ketiga yang menerima data?

9. Data Breach Notification — Notifikasi Kebocoran Data

Persyaratan: Jika terjadi kebocoran data (data breach), bisnis wajib memberitahu: (a) pengawas perlindungan data (Kominfo), dan (b) subjek data yang terpengaruh dalam waktu 3x24 jam.

- Siapkan prosedur respons insiden: siapa yang diberitahu, dalam urutan apa, dengan informasi apa
- Template notifikasi untuk subjek data
- Dokumentasi insiden: apa yang terjadi, data apa yang terpengaruh, langkah perbaikan

 Contoh notifikasi: 'Kami telah mendeteksi akses tidak sah ke database kami pada [tanggal]. Data yang terpengaruh meliputi [jenis data]. Kami telah mengambil langkah [langkah] untuk mengatasi masalah dan mencegah terulangnya. Hubungi [DPO] untuk informasi lebih lanjut.'

 Checklist: Apakah kamu punya prosedur untuk mendeteksi, merespons, dan memberitahu pihak yang terpengaruh saat terjadi kebocoran data?

10. Privacy Policy — Kebijakan Privasi

Persyaratan: Website yang mengumpulkan data pribadi WAJIB memiliki Privacy Policy yang jelas, lengkap, dan mudah diakses. Privacy Policy harus dalam Bahasa Indonesia (atau bilingual).

- Tersedia di footer website: link jelas ke /privacy-policy
- Ditulis dalam Bahasa Indonesia yang mudah dipahami (hindari bahasa hukum yang terlalu teknis)
- Mencakup semua 9 area di atas dalam satu dokumen
- Diperbarui setiap kali ada perubahan dalam pengumpulan atau pemrosesan data

 Gunakan template Privacy Policy yang compliant dari konsultan hukum atau platform hukum online Indonesia.

 Checklist: Apakah website kamu memiliki Privacy Policy yang lengkap, dalam Bahasa Indonesia, dan mudah diakses?

Ringkasan Checklist Kepatuhan UU PDP

#	Persyaratan	Apa yang Harus Ada	Status
1	Transparency	Privacy Policy lengkap dalam Bahasa Indonesia	□
2	Lawful Basis	Dasar hukum untuk setiap jenis data yang dikumpulkan	□
3	Consent	Checkbox persetujuan eksplisit di formulir	□
4	Data Rights	Kontak untuk menggunakan hak subjek data	□
5	DPO	Kontak penanggung jawab privasi di Privacy Policy	□
6	Security	HTTPS + security headers + 2FA admin	□
7	Cookie	Banner cookie dengan opsi tolak	□
8	3rd Party	Daftar vendor pihak ketiga di Privacy Policy	□
9	Breach Plan	Prosedur notifikasi kebocoran data	□
10	Privacy Policy	Privacy Policy terkini, accessible di footer	□

 Gunakan Security Audit dari ShortcutSistem (shortcutsistem.com/security-audit) untuk pengecekan otomatis terhadap aspek teknis keamanan website kamu sesuai standar OWASP.

Langkah Selanjutnya

1. Audit Website Sekarang
    - Buka shortcutsistem.com/security-audit
    - Jalankan Security Audit gratis
    - Periksa skor UU PDP Compliance di hasil audit
2. Perbaiki Privacy Policy
    - Gunakan checklist di atas sebagai panduan
    - Pastikan Privacy Policy dalam Bahasa Indonesia
    - Tambahkan kontak untuk hak subjek data
3. Pasang Cookie Banner
    - Pilih tools cookie consent (Termly, Cookiebot, atau alternatif gratis)

- Konfigurasi sesuai kategori: essential, analytics, marketing

4. Konsultasi Hukum (Jika Perlu)

- Untuk bisnis dengan volume data besar atau data sensitif, konsultasikan dengan ahli hukum IT/privasi data

---