Mematuhi UU PDP Indonesia: Solusi perlindungan data bisnis Anda

Perkuat keamanan data organisasi, pastikan kepatuhan terhadap regulasi, dan optimalkan praktik pengelolaan data Anda.



ManageEngine

Daftar Isi

Apa itu UU PDP? 4

Mengapa organisasi Anda harus mematuhi UU PDP? 5

Bagaimana TI membantu Anda mematuhi UU PDP. 8

Bagaimana ManageEngine dapat membantu organisasi Anda mematuhi UU PDP? 9

Pasal 4: Jenis Data Pribadi 11

Pasal 5: Prinsip Perlindungan Data Pribadi 17

Pasal 16: Pemrosesan Data Pribadi 24

Pasal 19: Pengendali dan Prosesor Data 28

Pasal 32: Perlindungan dan Pencegahan 34

Pasal 34: Penilaian Dampak Perlindungan Data 40

Pasal 35: Keamanan Data Pribadi 45

Pasal 36: Kerahasiaan Data Pribadi 51

Pasal 46: Pemberitahuan Pelanggaran Data 55

Pasal 51: Kewajiban Prosesor Data 59

Pasal 53: Pejabat yang Melaksanakan Fungsi Perlindungan Data Pribadi (DPO) 61

Pasal 54: Tugas Pejabat atau Petugas yang Melaksanakan Fungsi Perlindungan Data Pribadi (DPO) 65

Tentang ManageEngine 81

Disclaimer

Copyright © Zoho Corporation Pvt. Ltd. Seluruh hak cipta dilindungi undang-undang.
Materi ini ditujukan untuk memberikan gambaran umum tentang bagaimana Anda dapat menggunakan produk dan layanan ManageEngine dalam mengimplementasikan Undang-Undang Perlindungan Data Pribadi (UU PDP) di organisasi Anda. Kepatuhan penuh terhadap UU PDP memerlukan berbagai solusi, proses, sumber daya manusia, dan teknologi. Solusi yang disebutkan dalam Materi ini merupakan sebagian cara bagaimana tool manajemen TI dapat membantu memenuhi beberapa persyaratan dalam UU PDP.

Bersama dengan solusi, proses, dan sumber daya manusia yang tepat, solusi ManageEngine dapat membantu organisasi selaras dengan UU PDP. Namun, setiap organisasi wajib melakukan penilaian independen terkait fitur-fitur ManageEngine dan sejauh mana fitur tersebut dapat membantu dalam memenuhi ketentuan UU PDP.

Materi ini disediakan hanya untuk tujuan informasi dan tidak boleh dianggap sebagai nasihat hukum dalam menerapkan UU PDP. ManageEngine tidak memberikan jaminan, baik tersurat, tersirat, maupun berdasarkan undang-undang, serta tidak bertanggung jawab atas informasi yang terdapat dalam Materi ini.

Apa itu UU PDP?

UU Pelindungan Data Pribadi (UU PDP) adalah peraturan yang dirancang untuk melindungi data pribadi setiap individu di Indonesia. Undang-undang ini mengatur bagaimana organisasi mengelola dan memproses data pribadi secara aman, memastikan privasi, keamanan, dan transparansi dalam proses pengelolaan data.

Melalui kepatuhan terhadap UU PDP, perusahaan dapat meningkatkan kepercayaan pelanggan, mengurangi risiko pelanggaran data, dan menghindari sanksi hukum. UU Pelindungan Data Pribadi membantu menjaga integritas data pribadi, meningkatkan prosedur keamanan, serta menyelaraskan dengan standar perlindungan data global seperti GDPR.



Mengapa perusahaan harus mematuhi UU PDP?



Melindungi kepercayaan pelanggan dan reputasi

Mematuhi UU PDP membantu bisnis menjaga kepercayaan pelanggan dengan menunjukkan komitmen terhadap privasi dan keamanan data. Ketidakpatuhan dapat merusak reputasi dan mengurangi loyalitas pelanggan.



Menghindari sanksi hukum dan biaya

Gagal mematuhi UU PDP dapat menyebabkan denda berat dan tindakan hukum. Menghindari pelanggaran data juga mengurangi biaya hukum yang terkait dengan pelanggaran atau kebocoran data pribadi.



Menyesuaikan dengan standar perlindungan data global

Mematuhi UU PDP berarti bisnis memenuhi standar internasional, yang penting untuk kemitraan dan operasi global. Kepatuhan ini membuka peluang bisnis lebih luas di pasar global.

Bagaimana IT membantu Anda mematuhi UU Pelindungan Data Pribadi



Mapping dan inventarisasi data pribadi

Pastikan semua data pribadi yang dikelola organisasi teridentifikasi dengan jelas, termasuk lokasi penyimpanan dan alur aksesnya.



Memberikan visibilitas dan tool report real-time

Mendukung Pejabat Pelindungan Data (DPO) perusahaan Anda dengan menyediakan tool IT yang diperlukan untuk memantau akses data, menghasilkan laporan audit, dan memastikan kepatuhan.



Melakukan penilaian dampak pelindungan data (DPIA)

Menilai risiko terkait pemrosesan data pribadi untuk mengidentifikasi potensi dampak dan langkah mitigasi yang diperlukan.



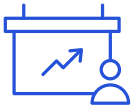
Keamanan dan perlindungan data yang terjamin

Mengamankan data pribadi dengan perlindungan seperti enkripsi, kontrol akses, dan pemantauan aktivitas yang mencurigakan.



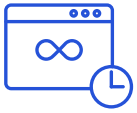
Pengembangan kebijakan internal

Membantu membangun kebijakan pengelolaan data pribadi yang jelas serta memastikan standar internal selalu sesuai dengan regulasi yang berlaku.



Memberikan pelatihan karyawan

Memberikan pelatihan reguler untuk meningkatkan kesadaran pegawai mengenai perlindungan data pribadi dan tanggung jawab mereka.



Monitoring dan audit akses data serta aktivitas pengguna

Melacak bagaimana data pribadi diakses dan digunakan, mengidentifikasi pelanggaran, serta memastikan kontrol keamanan efektif melalui audit dan pelaporan berkelanjutan.



Menangani insiden dan pelanggaran data

Mengidentifikasi dan merespons insiden keamanan dengan cepat. Memberitahukan individu yang terdampak dan otoritas terkait sesuai dengan UU PDP.

Bagaimana ManageEngine membantu perusahaan mematuhi UU PDP?


Log360
AD360
PAM360
Password Manager Pro
EventLog Analyzer
Endpoint DLP Plus
Endpoint Central
Patch Manager Plus
ServiceDesk Plus
DataSecurity Plus
Browser Security Plus
Produk apa saja yang membantu Anda mematuhi UU PDP?

Pasal

04

Jenis Data Pribadi

Mengklasifikasikan data pribadi menjadi data pribadi umum dan data pribadi spesifik.



DataSecurity Plus: Menemukan dan memelihara inventaris detail dari konten sensitif seperti PII dan ePHI yang tersebar di berbagai repositori data. Memindai nomor paspor, SSN, nomor kartu kredit, dan lebih dari 100 jenis data pribadi lainnya.



Endpoint DLP: Mencegah kebocoran data pribadi di seluruh perangkat endpoint.

Pasal

05

Prinsip Pelindungan Data Pribadi

Menetapkan prinsip dalam pemrosesan data pribadi, seperti perlindungan, kepastian hukum, kepentingan publik, pertanggungjawaban, dan kerahasiaan.



Log360: Membantu memastikan kerahasiaan data pribadi dengan memantau dan menganalisis log untuk mendeteksi adanya akses yang tidak sah.



EventLog Analyzer: Menganalisis log untuk mendeteksi aktivitas yang tidak sesuai dengan prinsip-prinsip tersebut.



Endpoint DLP: Mencegah kebocoran data melalui perangkat endpoint dan mengontrol transfer data yang tidak sah.



ServiceDesk Plus: Membantu mematuhi prinsip perlindungan data, termasuk transparansi dan pemrosesan data yang sah dengan menganonimkan data pribadi.



DataSecurity Plus: Memantau siapa yang mengakses data pribadi, termasuk kapan dan di mana data digunakan, serta menghapus file yang usang, duplikat, dan tidak memiliki owner untuk memastikan data tetap minimal dan efisien.



AD360: Menegakkan prinsip utama perlindungan data dengan memastikan manajemen identitas dan akses yang aman, akuntabel, dan patuh, dilengkapi dengan jejak audit terperinci serta kontrol akses.

Pasal

16

Pemrosesan Data Pribadi

Mengatur jenis pemrosesan data pribadi, termasuk pengumpulan, penyimpanan, dan penghapusan data.



EventLog Analyzer: Memantau aktivitas terkait pemrosesan data dan menjaga integritasnya.



DataSecurity Plus: Melindungi data dari akses yang tidak sah dan memastikan penghapusan data sesuai dengan regulasi.



AD360: Menerapkan kontrol akses yang ketat, akuntabilitas, serta tata kelola atas data pribadi.



Endpoint Central: Mengamankan endpoint tempat data pribadi disimpan dan diproses. Menerapkan langkah-langkah keamanan seperti enkripsi, kontrol akses, dan konfigurasi aman, untuk mendukung pemrosesan data yang aman di perangkat karyawan.



Patch Manager Plus: Menjaga keamanan sistem tempat data pribadi diproses dengan memastikan sistem operasi dan aplikasi selalu diperbarui dengan patch terbaru.

Pasal

19

Pengendali dan Prosesor Data Pribadi

Menetapkan kewajiban pengendali dan prosesor data pribadi dalam pemrosesan data pribadi.

Log360: Mendeteksi akses tidak sah atau aktivitas yang melanggar kebijakan pemrosesan, serta menyediakan laporan terperinci untuk memastikan data pribadi diproses sesuai dengan regulasi.

Pasal

32

Keamanan Data Pribadi

Menetapkan kewajiban bagi penyelenggara sistem elektronik untuk melaksanakan perlindungan data pribadi terhadap akses, perubahan, pengungkapan, atau penghancuran yang tidak sah.



EventLog Analyzer: Memantau dan menganalisis log untuk mendeteksi potensi pelanggaran keamanan data pribadi.



DataSecurity Plus: Menyediakan kontrol akses dan audit trail untuk memastikan hak akses yang tepat, sekaligus memantau setiap perubahan pada data pribadi.



Browser Security Plus: Mengamankan penggunaan browser dengan kebijakan kontrol yang membatasi unduhan dan akses tidak sah.



PAM360: Memastikan kontrol akses yang ketat untuk akun dengan hak istimewa, serta merekam sesi guna meningkatkan keamanan pemantauan akses data pribadi.



Password Manager Pro: Mengelola dan menyimpan kredensial secara aman, sekaligus memastikan kontrol akses yang tepat terhadap data pribadi yang tersimpan dalam sistem.

Log360: Menjaga keamanan data pribadi dengan memantau log untuk akses tidak sah serta menyediakan laporan terperinci guna mendeteksi potensi pelanggaran.

Endpoint Central: Melindungi data di seluruh perangkat dengan kebijakan keamanan yang tepat, memastikan data pribadi di endpoint terlindungi dari akses tidak sah, perubahan, maupun kebocoran.

AD360: Melindungi data pribadi dengan MFA, kebijakan akses bersyarat, audit, dan peninjauan akses berkala.

Pasal

34

Data Protection Impact Assessment

Mengatur kewajiban untuk melakukan data protection impact assessment pada pemrosesan data pribadi yang berisiko tinggi.



AD360: Memberikan visibilitas terhadap aktivitas pengguna dan celah kepatuhan. Memantau, mendeteksi, dan melaporkan akses tidak sah terhadap data pribadi yang dikelola oleh prosesor data.



Log360: Menyediakan UEBA dan deteksi insiden secara real-time untuk mengidentifikasi serta merespons upaya akses tidak sah dan perilaku anomali dengan cepat dan efektif.

Pasal

35

Keamanan Data Pribadi

Menetapkan kewajiban untuk melindungi dan memastikan keamanan data pribadi selama proses pemrosesan.

EventLog Analyzer: Menyediakan pemantauan dan pelaporan insiden terkait keamanan data pribadi.

DataSecurity Plus: Memastikan kontrol akses dan melindungi integritas data pribadi.

Patch Manager Plus: Memastikan perlindungan berkelanjutan sistem yang terlibat dalam pemrosesan data pribadi dengan mengotomatisasi penerapan patch di seluruh OS dan aplikasi pihak ketiga.

AD360: Memastikan keamanan data pribadi sepanjang siklus pemrosesan dengan menegakkan kontrol akses, memantau aktivitas pengguna, dan menghasilkan pemberitahuan real-time untuk mencegah akses yang tidak sah atau pelanggaran data.

Pasal

36

Kerahasiaan Data Pribadi

Mengharuskan pengendali data untuk menjaga kerahasiaan data pribadi yang diproses.



DataSecurity Plus: Melindungi kerahasiaan data dengan kontrol akses yang ketat.



Password Manager Pro: Menyimpan dan mengelola kata sandi dengan aman untuk menjaga kerahasiaan data pribadi.



Endpoint Central: Memastikan data pribadi di endpoint tetap terjaga kerahasiaannya. Menerapkan kebijakan enkripsi perangkat, mengelola kontrol akses, dan memastikan data sensitif tersimpan dengan aman.



ServiceDesk Plus: Menerapkan teknik anonimisasi untuk melindungi informasi sensitif sesuai dengan persyaratan kerahasiaan UU PDP.



AD360: Menerapkan kontrol akses yang granular, mengaktifkan pemantauan real-time, dan melakukan auditing menyeluruh untuk membantu data controller memenuhi persyaratan kerahasiaan data.

Pasal

46

Pemberitahuan Pelanggaran Data Pribadi

Mengatur kewajiban untuk memberitahukan subjek data dan otoritas terkait jika terjadi pelanggaran data pribadi.

Log360: Memberikan laporan real-time dan pemberitahuan tentang pelanggaran data pribadi.

EventLog Analyzer: Membantu mendeteksi dan melaporkan pelanggaran data untuk kepatuhan.

AD360: Menawarkan pemberitahuan real-time, laporan penilaian risiko yang terperinci, dan log audit untuk memastikan deteksi dan pemberitahuan pelanggaran data pribadi secara tepat waktu.

Pasal

51

Kewajiban Prosesor Data Pribadi

Menetapkan kewajiban prosesor data dalam memproses data sesuai dengan instruksi pengendali.

AD360: Memantau akses pengguna di Active Directory, mendeteksi serta melaporkan akses tidak sah terhadap data yang dikelola oleh data processor.

Pasal

53

Pejabat atau Petugas yang Melaksanakan Fungsi Pelindungan Data Pribadi (DPO)

Mengatur kewajiban pengendali dan prosesor untuk menunjuk DPO yang bertugas memantau dan memastikan kepatuhan terhadap UU PDP.

PAM360: Mengelola akses istimewa untuk pengguna dengan hak akses tingkat tinggi, termasuk sesi akses yang diaudit untuk memastikan kepatuhan oleh DPO.

Pasal

54

Tugas Pejabat atau Petugas Pelindungan Data Pribadi (DPO)

Mengatur tugas DPO untuk memantau kepatuhan terhadap UU PDP, memberikan saran, serta bertindak sebagai penghubung antara organisasi dan otoritas terkait.

Log360: Membantu DPO memantau dan menganalisis log aktivitas data pribadi untuk memastikan kepatuhan terhadap kebijakan dan regulasi yang berlaku.

EventLog Analyzer: Memfasilitasi analisis log dan pelaporan insiden, yang berguna bagi DPO untuk memastikan pemrosesan data pribadi sesuai dengan regulasi.

Tentang ManageEngine

ManageEngine menghadirkan rangkaian solusi manajemen IT terlengkap di industri. Dengan lebih dari 60 produk, kami memiliki semua yang Anda perlukan untuk mengelola operasional IT Anda. Mulai dari jaringan dan server hingga aplikasi, service desk, Active Directory, keamanan, desktop, dan mobile.

Sejak tahun 2002, tim IT terbaik Anda telah memilih software kami yang terjangkau, kaya fitur, dan mudah digunakan.

Saat Anda bersiap menghadapi tantangan manajemen IT di masa depan, kami siap memimpin dengan solusi terbaru, integrasi kontekstual, dan inovasi yang hanya bisa diberikan oleh perusahaan yang berfokus pada pelanggan. Sebagai bagian dari Zoho Corporation, kami terus mendorong keselarasan bisnis dan IT yang akan membantu Anda meraih peluang masa depan.



Ambil kendali IT Anda.

Pantau, kelola, dan amankan enterprise digital Anda dengan ManageEngine



Kelola akses dan identitas digital

Kelola dan amankan identitas digital di seluruh organisasi Anda dengan identity orchestration, privileged access security, CIEM, MFA, SSO, role-based access control, dan lainnya. manageengine.com/iam

Kendalikan dan amankan setiap endpoint

Kelola dan amankan seluruh endpoint di berbagai fungsi, mulai dari end-user computing, cybersecurity, governance, risk & compliance (GRC), hingga I/O dan lainnya.
manageengine.com/uems

Tingkatkan keamanan & kepatuhan IT

Deteksi, investigasi, dan respons cepat terhadap ancaman keamanan dengan UEBA, threat intelligence, dan log monitoring. Penuhi standar kepatuhan serta minimalkan risiko dengan laporan yang siap audit.
manageengine.com/siem

Optimalkan IT dengan aplikasi low-code
Tingkatkan kemampuan proses IT dengan menggabungkan low-code dan GenAI. Selesaikan tantangan IT dengan cepat, berinovasi tanpa banyak coding, dan jadikan organisasi Anda lebih lincah.
manageengine.com/lowcode

Hadirkan pengalaman layanan yang cerdas
Tingkatkan workflow layanan Anda dengan best practice ITSM yang direkomendasikan industri, orkestrasi yang tangguh, dan kapabilitas AI native.
manageengine.com/usm

Perkuat jaringan & operasional IT
Dapatkan visibilitas menyeluruh atas jaringan dan aplikasi dengan observabilitas berbasis AI. Proaktif dalam menyelesaikan masalah, optimalkan performa, dan tingkatkan keamanan IT Anda.
manageengine.com/itom

Insight terpadu untuk seluruh IT
Visualisasikan seluruh aspek IT dengan mudah. Dengan decision intelligence, identifikasi risiko sejak dini, atasi hambatan operasional, dan terapkan strategi kontekstual yang praktis.
manageengine.com/ita