JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1430-1438

Analisis Kepatuhan UU PDP Melalui Penerapan *Privacy by Design* pada Pengembangan Sistem Informasi

Zuhud Qolbu Adi[1], Evy Nurmiati[2]

[1,2]Fakultas Sains dan Teknologi, Sistem Informasi, Universitas Islam Negeri Syarif Hidayatullah Jakarta, Indonesia
Email: [1*]zuhud.qolbu24@mhs.uinjkt.ac.id, [2]evy.nurmiati@uinjkt.ac.id
(* : coressponding author)

Abstrak−Maraknya insiden kebocoran data pribadi di Indonesia, mulai dari BPJS Kesehatan (2021), KPU (2023), Bank Syariah Indonesia (2023), hingga Pusat Data Nasional (2024) telah mempertegas urgensi perlindungan data sebagai isu fundamental dalam ekosistem digital nasional. Penelitian ini bertujuan menganalisis implementasi prinsip *Privacy by Design* (PbD) sebagai strategi etis dan teknis dalam memenuhi kepatuhan terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Metode yang digunakan adalah studi literatur kualitatif dengan pendekatan yuridis-normatif yang membandingkan tujuh prinsip fondasi PbD dengan kewajiban pengendali data dalam regulasi nasional, standar internasional ISO/IEC 29100, GDPR Eropa, serta kode etik ACM dan IEEE. Hasil kajian menunjukkan korelasi sistematis antara prinsip PbD dan pasal-pasal UU PDP yang membuktikan bahwa integrasi privasi sejak fase inisiasi sistem dapat meminimalisir risiko hukum dan teknis secara signifikan. Penelitian ini turut mengidentifikasi tiga hambatan utama implementasi PbD di Indonesia, yakni keterbatasan literasi regulasi, budaya organisasi profit, dan kompleksitas sistem warisan (*legacy systems*). Sebagai kontribusi praktis, diusulkan kerangka integrasi PbD dalam siklus hidup pengembangan perangkat lunak (SDLC) yang memetakan setiap tahapan pengembangan terhadap kewajiban spesifik UU PDP. Kesimpulan menegaskan bahwa penerapan PbD merupakan manifestasi profesionalisme dan integritas etis praktisi teknologi informasi dalam melindungi hak asasi pengguna di era digital.

Kata Kunci: Etika Profesi; ISO/IEC 29100, Keamanan Data; *Privacy by Design*; SDLC; Sistem Informasi

Abstract−*The wave of personal data breaches in Indonesia—including incidents at BPJS Kesehatan (2021), KPU (2023), Bank Syariah Indonesia (2023), and the National Data Center (2024)—has underscored the critical urgency of data protection as a foundational issue within the national digital ecosystem. This study aims to analyze the implementation of Privacy by Design (PbD) principles as an ethical and technical strategy for achieving compliance with Law Number 27 of 2022 on Personal Data Protection (UU PDP). The research employs a qualitative literature study with a juridical-normative approach, systematically comparing the seven foundational PbD principles with the obligations of data controllers under national regulations, international standard ISO/IEC 29100, the EU GDPR, and the professional codes of ACM and IEEE. The findings demonstrate a systematic correlation between PbD principles and specific UU PDP articles, confirming that proactive privacy integration from the system initiation phase significantly minimizes both legal and technical risks. The study also identifies three primary barriers to PbD implementation in Indonesia: limited regulatory literacy, profit-oriented organizational culture, and the complexity of legacy systems. As a practical contribution, a PbD integration framework mapped to the Software Development Life Cycle (SDLC) is proposed, aligning each development phase with specific UU PDP obligations. The conclusion affirms that PbD adoption constitutes a manifestation of the professionalism and ethical integrity of information technology practitioners in protecting users' fundamental rights in the digital era.*

Keywords: *Data Security; Information Systems; Personal Data Protection Law; Privacy by Design; Professional Ethics*

1. PENDAHULUAN

Di era transformasi digital yang masif, data telah bertransformasi menjadi aset strategis paling bernilai dalam ekosistem ekonomi global, sehingga kerap dijuluki sebagai "*the new oil*" (Zuboff, 2019). Dalam ekosistem Sistem Informasi (SI), pengolahan data pribadi menjadi fondasi utama dalam penyediaan layanan yang personal dan efisien. Namun, peningkatan nilai data ini berbanding lurus dengan risiko keamanan yang semakin kompleks. Praktik pengembangan sistem modern sering kali terjebak pada pemenuhan fungsionalitas dan kecepatan rilis produk semata, sementara perlindungan privasi kerap dikesampingkan sebagai aspek sekunder dalam siklus hidup pengembangan perangkat lunak (SDLC).

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1430-1438

Indonesia tidak luput dari ancaman serius terkait perlindungan data pribadi. Dalam kurun waktu 2021–2024, serangkaian insiden kebocoran data skala besar telah mengguncang kepercayaan publik. Kebocoran data BPJS Kesehatan pada tahun 2021 yang mengekspos data 279 juta penduduk, diikuti dugaan kebocoran data 204 juta pemilih KPU pada 2023, serangan ransomware LockBit terhadap Bank Syariah Indonesia yang berdampak pada 15 juta nasabah, serta lumpuhnya Pusat Data Nasional (PDN) pada 2024 akibat serangan siber, merupakan bukti nyata bahwa praktik keamanan data di Indonesia masih berada pada level yang mengkhawatirkan (Ramadhani & Kurniawan, 2024). Fenomena ini diperparah oleh modus kejahatan siber yang semakin canggih, mulai dari manipulasi input tradisional hingga serangan berbasis kecerdasan buatan yang sulit dideteksi tanpa kontrol manajerial sistematis.

Sebagai respons terhadap urgensi tersebut, Pemerintah Indonesia secara resmi mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)—merupakan regulasi perlindungan data pertama yang bersifat komprehensif di Indonesia. UU ini menetapkan standar kepatuhan yang ketat bagi pengendali dan prosesor data, dengan ancaman sanksi administratif hingga pidana bagi pelanggaran. Kehadiran UU PDP menuntut redefinisi profesionalisme bagi praktisi Teknologi Informasi (TI), di mana kepatuhan hukum kini menjadi bagian integral dari tanggung jawab etis profesi. Namun, tanpa panduan teknis yang konkret, banyak praktisi TI yang masih bingung dalam menerjemahkan kewajiban hukum ke dalam praktik pengembangan sistem sehari-hari.

Meskipun regulasi telah tersedia, terdapat kesenjangan (*gap*) besar dalam implementasi teknis di lapangan. Banyak praktisi TI yang masih menerapkan keamanan data sebagai fitur tambahan (*add-on*) yang dipasang setelah sistem selesai dibangun, bukan sebagai bagian dari rancangan awal—sebuah pendekatan yang oleh Cavoukian (2009) disebut sebagai "reaktif" dan secara inheren rentan. Hal ini bertentangan dengan prinsip etika profesi yang diatur dalam Kode Etik ACM (2018) dan IEEE (2014), yang menempatkan keselamatan dan kesejahteraan pengguna sebagai prioritas tertinggi. Oleh karena itu, artikel ini mengusulkan *Privacy by Design* (PbD) sebagai standar kerja etis yang menawarkan pendekatan proaktif dalam mengintegrasikan privasi ke dalam arsitektur sistem sejak tahap inisiasi.

Penelitian ini memiliki tiga tujuan spesifik: (1) menganalisis korelasi sistematis antara tujuh prinsip PbD dan pasal-pasal kewajiban dalam UU PDP; (2) mengidentifikasi tantangan utama implementasi PbD oleh praktisi TI di Indonesia; dan (3) merumuskan kerangka kerja integratif PbD dalam SDLC yang dapat dijadikan panduan praktis bagi pengembang sistem informasi. Kontribusi teoritis penelitian ini terletak pada pemetaan standar internasional ke dalam konteks hukum positif Indonesia yang belum banyak dibahas dalam literatur nasional.

2. METODE

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan yuridis-normatif. Metode ini dipilih karena permasalahan yang dikaji berada di persimpangan antara disiplin ilmu teknologi informasi, hukum, dan etika profesi—tiga domain yang memerlukan analisis tekstual dan komparatif mendalam terhadap dokumen primer dan sekunder.

2.1 Tahapan Penelitian (Workflow)

Tahapan penelitian disusun secara sistematis untuk menjamin validitas hasil analisis. Alur kerja penelitian ini mengikuti langkah-langkah berikut:

a. Identifikasi masalah: **:** Menganalisis fenomena kebocoran data pribadi di Indonesia dan tantangan etika bagi praktisi Sistem Informasi, dengan mengkaji laporan insiden dari BSSN, Kominfo, dan media teknologi terpercaya (2020–2024).
b. Pengumpulan data: Melakukan studi pustaka komprehensif terhadap prinsip Privacy by Design (PbD), Kode Etik ACM/IEEE, literatur manajemen keamanan August Beguai, standar ISO/IEC 29100, Scopus/SINTA yang diterbitkan dalam 5 tahun terakhir.
c. Analisis komparatif: Memetakan korelasi antara 7 prinsip PbD dengan kewajiban pengendali data dalam UU PDP, serta membandingkan regulasi Indonesia dengan GDPR sebagai tolak ukur internasional terkemuka.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1430-1438

d. Analisis Tantangan: Mengidentifikasi hambatan implementasi PbD di Indonesia berdasarkan kajian laporan industri, studi kasus insiden keamanan, dan penelitian empiris terkini.
e. Sintesis solusi: Merumuskan kerangka kerja etis bagi praktisi TI dengan mengintegrasikan prinsip PbD ke dalam setiap fase SDLC, dilengkapi pemetaan terhadap kewajiban spesifik UU PDP.

2.2 Instrumen Analisis Penelitian

Untuk mempermudah pemetaan data, penelitian ini menggunakan instrumen analisis yang merujuk pada standar baku internasional dan nasional seperti yang ditunjukkan pada Tabel 1.

Tabel 1. Instrumen Analisis Kepatuhan dan Etika Privasi

Komponen Analisis	Referensi Utama	Parameter Utama
Standar Teknis	*Privacy by Design* (PbD)	7 Prinsip Fondasi Privasi Proaktif
Regulasi Nasional	UU No. 27 Tahun 2022 (UU PDP)	Kewajiban Pengendali & Prosesor Data
Landasan Etika	Kode Etik ACM & IEEE	Integritas dan Tanggung Jawab Profesional
Kontrol Manajerial	August Beguai (1983)	Pencegahan Kejahatan melalui Audit Internal
Standar Internasional	ISO/IEC 29100 & GDPR	Privacy Framework & Data Profection Principles

Sumber: Diolah dari berbagai referensi, 2025

3. HASIL DAN PEMBAHASAN

3.1 Konteks: Lanskap Ancaman Keamanan Data di Indonesia

Sebelum membahas solusi teknis, penting untuk memahami konteks dan skala permasalahan yang dihadapi Indonesia. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN) tahun 2023, Indonesia mencatat lebih dari 361 juta anomali lalu lintas siber, dengan insiden ransomware dan pencurian data sebagai ancaman dominan. Tabel 2 merangkum insiden kecoboran data signifikan yang terjadi dalam beberapa tahun terakhir.

Tabel 2. Insiden Kebocoran Data Signifikan di Indonesia (2021-2024)

Instansi/Entitas	Tahun / Skala	Dampak
BPJS Kesehatan	2021 / ±279 juta rekam	Kebocoran NIK, nomor KK, dan data medis jutaan warga
KPU (e-KTP)	2023 / ±204 juta rekam	Dugaan kebocoran data pemilih nasional berisi identitas lengkap
Bank Syariah Indonesia (BSI)	2023 / ±15 juta nasabah	Ransomware LockBit, gangguan layanan & kebocoran data nasabah
Pusat Data Nasional (PDN)	2024 / Skala nasional	Serangan ransomware pada infrastruktur pemerintah pusat
IndiHome / Telkom	2023 / ±26 juta data	Data riwayat browsing pelanggan bocor ke forum dark web

Sumber: Diolah dari laporan BSSN, media teknologi, dan penelitian terkini, 2025

Pola yang konsisten dari seluruh insiden di atas adalah absennya mekanisme perlindungan privasi yang bersifat proaktif dan terintegrasi. Sebagian besar sistem yang terkena dampak dibangun dengan paradigma lama di mana keamanan merupakan lapisan terakhir yang ditambahkan—bukan fondasi yang membangun seluruh arsitektur sistem. Kondisi ini secara langsung menggarisbawahi urgensi adopsi Privacy by Design sebagai perubahan paradigma mendasar dalam praktik pengembangan sistem informasi di Indonesia.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1430-1438

3.2 Privacy by Design: Konsep, Sejarah, dan Relevansi Global

Privacy by Design (PbD) adalah sebuah kerangka kerja yang dikembangkan oleh Dr. Ann Cavoukian, mantan Komisioner Informasi dan Privasi Provinsi Ontario, Kanada, pada tahun 1995 dan kemudian dipublikasikan secara formal pada tahun 2009 (Cavoukian, 2009). Konsep ini lahir dari kesadaran bahwa teknologi informasi yang semakin canggih membawa risiko privasi yang tidak dapat diselesaikan hanya melalui regulasi dan kepatuhan pasca-insiden. PbD menawarkan pendekatan yang lebih fundamental: privasi harus diintegrasikan ke dalam teknologi, praktik bisnis, dan desain fisik sejak awal, bukan ditempelkan setelahnya.

Pada tingkat internasional, PbD telah mendapatkan pengakuan yang signifikan. General Data Protection Regulation (GDPR) Uni Eropa—yang dianggap sebagai regulasi perlindungan data paling komprehensif di dunia—secara eksplisit mewajibkan prinsip "data protection by design and by default" dalam Pasal 25 (European Parliament, 2016). Hal serupa juga tercermin dalam standar internasional ISO/IEC 29100:2011 (Privacy Framework), yang memberikan kerangka terminologi dan prinsip tingkat tinggi untuk perlindungan informasi identitas pribadi dalam sistem TIK. Adopsi global ini membuktikan bahwa PbD bukan sekadar konsep akademis, melainkan standar industri yang telah terbukti efektif.

PbD berdiri di atas tujuh prinsip fondasi yang saling melengkapi: (1) Proaktif, bukan reaktif; (2) Privasi sebagai pengaturan standar; (3) Privasi yang tertanam dalam desain; (4) Fungsionalitas penuh tanpa kompromi; (5) Keamanan ujung ke ujung; (6) Visibilitas dan transparansi; serta (7) Penghormatan terhadap privasi pengguna. Ketujuh prinsip ini bukanlah daftar teknis, melainkan filosofi holistik yang mengubah cara pandang praktisi TI terhadap privasi: dari beban regulasi menjadi nilai tambah produk.

3.3 Analisis Komparatif: Pemetaan Prinsip PbD terhadap UU PDP

Implementasi Privacy by Design bukan sekedar pilihan teknis, melainkan kewajiban etis yang kini memiliki landasan hukum kuat di Indonesia melalui UU PDP. Berdasarkan hasil analisis komparatif, ditemukan korelasi yang sangat signifikan antara standar internasional PbD dengan pasal-pasal kewajiban pengendali data. Pemetaan lengkap disajikan dalam Tabel 3.

Tabel 3. Pemetaan Prinsip PbD terhadap Pasal UU PDP No.27 Tahun 2022

Prinsip Privacy by Design	Pasal UU PDP Terkait	Relevansi Etika Profesi
Proactive, not Reactive	Pasal 34 (Penilaian Dampak)	Pencegahan risiko privasi secara dini sebelum sistem diluncurkan
Privacy as Default	Pasal 35 (Langkah Teknis)	Perlindungan otomatis tanpa intervensi pengguna
Embedded into Design	Pasal 16 (Tujuan Spesifik)	Privasi terintegrasi sejak arsitektur awal, bukan tambahan akhir
Full Functionality	Pasal 47(Keamanan Pemrosesan)	Keseimbangan antara keamanan data dan kegunaan sistem
End-to-End Security	Pasal 39 (Penghapusan Data)	Keamanan mencakup seluruh siklus hidup data
Visibility & Transparency	Pasal 21 (Informasi Pemrosesan)	Akuntabilitas penuh kepada subjek data dan publik
User-Centric	Pasal 5-11 (Hak Subjel Data	Penghormatan atas otonomi dan hak asasi pengguna

Sumber: Diolah dari Cavoukian (2009) dan UU No. 27 Tahun 2022

3.3.1 Proaktif dan Preventif (Bukan Reaktif)

Prinsip pertama PbD mengharuskan praktisi TI untuk mengantisipasi risiko privasi sebelum insiden terjadi. Hal ini selaras dengan Pasal 34 UU PDP yang mewajibkan pengendali data untuk melaksanakan Data Protection Impact Assessment (DPIA) apabila pemrosesan data memiliki risiko tinggi bagi subjek data. DPIA bukan sekadar dokumen administratif; ia adalah proses analitik yang mengidentifikasi, menilai, dan memitigasi risiko privasi sejak tahap

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1430-1438

perencanaan. Dalam konteks kode etik ACM (2018), prinsip ini mencerminkan nilai "avoiding harm"—kewajiban aktif untuk mencegah kerugian yang dapat diperkirakan, bukan sekadar merespons setelah kerusakan terjadi.

3.3.2 Privasi sebagai Pengaturan Standar (Default Setting)

PbD menetapkan bahwa perlindungan data harus menjadi pengaturan bawaan (*default*) tanpa perlu tindakan tambahan dari pengguna. Prinsip ini sejalan dengan GDPR Pasal 25 yang mewajibkan "data protection by default", dan dalam konteks UU PDP diterjemahkan dalam Pasal 35 sebagai kewajiban pengendali untuk menyusun dan menerapkan langkah teknis pengamanan. Implikasi praktisnya sangat konkret: sistem harus dikonfigurasikan untuk mengumpulkan hanya data yang minimum, mematikan berbagi data dengan pihak ketiga secara default, dan memastikan bahwa pengaturan privasi tertinggi adalah pengaturan awal tanpa intervensi pengguna (Waldman, 2018).

3.3.3 Privasi yang Terintegrasi dalam Desain

Privasi tidak boleh diperlakukan sebagai "fitur tambahan" (*add-on*) yang ditempel setelah sistem selesai. Prinsip ini merupakan inti dari PbD dan berkorelasi langsung dengan Pasal 16 UU PDP yang mengatur prinsip data minimization—bahwa data hanya boleh dikumpulkan untuk tujuan yang spesifik, eksplisit, dan sah. Dalam perspektif August Beguai (1983), pendekatan holistik terhadap keamanan sistem informasi mensyaratkan bahwa kontrol keamanan harus bersifat inherent, bukan instrumental. Hal ini juga selaras dengan prinsip "secure by design" yang dipromosikan oleh National Institute of Standards and Technology (NIST) dalam kerangka Cybersecurity Framework-nya (NIST, 2018).

3.3.4 Fungsionalitas Penuh, Keamanan Ujung ke Ujung, dan Transparansi

Prinsip keempat hingga keenam PbD menyangkut aspek operasional dan akuntabilitas. Prinsip fungsionalitas penuh menegaskan bahwa privasi dan kegunaan sistem bukanlah trade-off—keduanya dapat dicapai secara simultan (Pasal 47 UU PDP). Keamanan ujung ke ujung (Pasal 39) berarti perlindungan data mencakup seluruh siklus hidupnya, dari pengumpulan hingga penghapusan yang terverifikasi. Sementara itu, prinsip transparansi yang berkorelasi dengan Pasal 21 UU PDP mewajibkan pengendali untuk memberikan informasi yang jelas, akurat, dan mudah diakses mengenai praktik pemrosesan data. Menurut Nissenbaum (2020), transparansi adalah fondasi kepercayaan publik terhadap sistem digital—tanpa transparansi, legitimasi sosial dari teknologi informasi terancam.

3.4 Perbandingan dengan Regulasi Internasional: GDPR sebagai Tolok Ukur

Perbandingan antara UU PDP Indonesia dan GDPR Eropa memberikan perspektif penting mengenai kematangan regulasi perlindungan data Indonesia. Secara struktural, UU PDP memiliki kesamaan mendasar dengan GDPR dalam aspek prinsip pemrosesan yang sah, hak subjek data, kewajiban pemberitahuan pelanggaran, dan sanksi yang signifikan. Namun, terdapat beberapa area di mana UU PDP masih perlu penguatan.

GDPR secara eksplisit mewajibkan Data Protection Officer (DPO) bagi kategori tertentu pengendali data dan menetapkan kewajiban DPIA yang lebih rinci. UU PDP, meskipun mengamanatkan pejabat yang bertanggung jawab atas perlindungan data (Pasal 53), belum memiliki panduan teknis sedetail GDPR. Kesenjangan ini menciptakan peluang bagi Indonesia untuk belajar dari pengalaman implementasi GDPR di Eropa, khususnya dalam hal standardisasi protokol teknis dan pembentukan otoritas pengawas yang independen dan berdaya (Lukito, 2023). Dalam hal ini, PbD berfungsi sebagai jembatan teknis yang membantu praktisi TI di Indonesia memenuhi tidak hanya standar lokal, tetapi juga mempersiapkan sistem mereka untuk beroperasi dalam ekosistem global yang semakin ketat regulasinya.

3.5 Tantangan Implementasi PbD bagi Praktisi TI di Indonesia

Meskipun prinsip PbD menawarkan kerangka kerja yang ideal, implementasinya di lapangan menghadapi berbagai tantangan kompleks yang bersifat teknis, kultural, dan struktural. Berdasarkan analisis terhadap ekosistem teknologi di Indonesia, terdapat tiga hambatan utama yang perlu diatasi.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1430-1438

3.5.1 Keterbatasan Literasi Regulasi dan Kompetensi Privasi

Banyak pengembang perangkat lunak di Indonesia memiliki kemahiran teknis tinggi namun masih minim pemahaman mengenai aspek hukum teknologi, khususnya UU PDP. Survei yang dilakukan Nasution & Sari (2023) terhadap 150 praktisi TI di Indonesia menunjukkan bahwa hanya 34% responden yang memiliki pemahaman memadai tentang kewajiban UU PDP, dan hanya 18% yang pernah melakukan DPIA dalam proyek mereka. Tanpa literasi hukum yang memadai, praktisi cenderung mengabaikan prinsip Privacy as Default karena dianggap menambah beban kerja koding dan menghambat kecepatan rilis produk (speed-to-market). Solusi untuk tantangan ini memerlukan rekonstruksi kurikulum pendidikan TI yang mengintegrasikan mata kuliah etika dan hukum teknologi, serta insentif sertifikasi privasi profesional seperti Certified Information Privacy Professional (CIPP) yang diakui secara internasional.

3.5.2 Budaya Organisasi dan Biaya Implementasi yang Dipersepsikan Tinggi

Penerapan PbD membutuhkan investasi waktu dan sumber daya yang lebih besar sejak tahap awal perancangan sistem. Dalam ekosistem startup dan perusahaan teknologi berorientasi pertumbuhan cepat, tekanan untuk menghasilkan produk minimal yang dapat dipasarkan (Minimum Viable Product/MVP) sering mengalahkan pertimbangan privasi. Beguai (1983) telah lama memperingatkan bahwa lemahnya kontrol manajerial dalam struktur organisasi adalah akar dari banyak kegagalan keamanan informasi. Namun, perspektif ini perlu direvisi: studi IBM (2023) menemukan bahwa rata-rata biaya kebocoran data secara global mencapai USD 4,45 juta per insiden—angka yang jauh melampaui investasi awal dalam infrastruktur privasi yang kuat. Dengan demikian, PbD harus diposisikan bukan sebagai biaya, melainkan sebagai investasi perlindungan reputasi dan kelangsungan bisnis jangka panjang.

3.5.3 Kompleksitas Sistem Warisan (Legacy Systems)

Tantangan ketiga dan mungkin paling kompleks secara teknis adalah integrasi prinsip PbD ke dalam sistem informasi yang sudah berjalan dan tidak dirancang dengan standar privasi modern. Fenomena ini sangat relevan bagi instansi pemerintah dan perusahaan BUMN di Indonesia yang masih mengoperasikan infrastruktur TI yang dibangun sebelum era kesadaran privasi. Melakukan *retrofitting* atau modernisasi sistem warisan memerlukan pendekatan bertahap yang dikenal sebagai "privacy debt remediation"—proses sistematis mengidentifikasi, memprioritaskan, dan mengeliminasi kerentanan privasi yang terakumulasi dari praktik pengembangan lama (Ferdiana, 2022). Proses ini menuntut kreativitas tinggi dari praktisi TI untuk merancang solusi mitigasi yang efektif tanpa mengorbankan fungsionalitas sistem yang sudah ada.

3.6 Kerangka Kerja Integratif: PbD dalam Siklus Hidup Pengembangan Sistem (SDLC)

Sebagai kontribusi praktis utama penelitian ini, berikut disajikan kerangka kerja integratif yang memetakan penerapan prinsip PbD ke dalam setiap fase Siklus Hidup Pengembangan Perangkat Lunak (SDLC). Kerangka ini dirancang untuk membantu praktisi TI menerjemahkan kewajiban abstrak UU PDP menjadi tindakan teknis yang konkret dan terverivikasi.

Tabel 4. Kerangka Integrasi PbD dalam SDLC dan Korelasi dengan UU PDP

Fase SDLC	Praktik PbD yang Direkomendasikan	Pasal UU PDP yang Dipenuhi
Requirement Analysis	Penilaian dampak privasi (DPIA), identifikasi data minimal yang dibutuhkan	Pasal 34 (Penilaian Dampak)
System Design	Arsitektur privasi-pertama, enkripsi end-to-end, pseudonimisasi data sensitif	Pasal 35 & 47 (Langkah Teknis & Keamanan)
Development	Secure coding standards, minimasi pengumpulan data, kontrol akses berbasis peran	Pasal 16 & 39 (Tujuan Spesifik & Penghapusan)

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1430-1438

Testing	Privacy penetration testing, validasi kebijakan retensi data	Pasal 21 (Akuntabilitas Pemrosesan)
Deployment & Opeations	Audit berkala, monitoring keamanan, mekanisme pelaporan insiden	Pasal 46 (Pemberitahuan Kegagalan Keamanan)
Retirement / End-of-Life	Penghapusan data terverifikasi, pencabutan izin akses, pemusnahan aset digital	Pasal 39 (Penghapusan & Pemusnahan Data)

Sumber: Diolah dari Cavoukian (2009), Putra & Wiguna (2021), dan UU No. 27 Tahun 2022

Kerangka pada Tabel 4 menunjukkan bahwa kepatuhan terhadap UU PDP bukanlah aktivitas tunggal yang dilakukan pada satu titik waktu, melainkan proses berkelanjutan yang terintegrasi dalam seluruh siklus hidup sistem. Pendekatan ini juga sejalan dengan konsep DevSecOps dalam rekayasa perangkat lunak modern, di mana keamanan (dan privasi) diintegrasikan sejak tahap paling awal pengembangan, bukan sebagai pemeriksaan akhir sebelum deployment (Kim et al., 2019). Penggunaan alat bantu seperti Privacy Impact Assessment (PIA) toolkit, automated privacy testing frameworks, dan data flow mapping tools dapat memfasilitasi implementasi kerangka kerja ini secara lebih efisien.

3.7 Etika Profesi sebagai Fondasi: Perspektif ACM, IEEE, dan Teori Profesionalisme

Dimensi etika profesi merupakan lapisan yang tidak dapat dipisahkan dari diskusi teknis dan hukum mengenai PbD. Kode Etik ACM (2018) dalam Prinsip 1.6 secara eksplisit menyatakan bahwa profesional komputasi harus "hormati privasi" dan hanya mengumpulkan data minimum yang diperlukan untuk fungsi yang sah. Lebih jauh, Kode Etik IEEE (2014) mengharuskan anggotanya untuk "melindungi keselamatan, kesehatan, dan kesejahteraan publik"—yang dalam konteks digital mencakup perlindungan data pribadi sebagai komponen kesejahteraan fundamental.

Zulkarnain (2023) berargumen bahwa dilema etika terbesar yang dihadapi pengembang sistem saat ini adalah tekanan konflik antara tuntutan bisnis (kecepatan pengembangan, monetisasi data) dan kewajiban profesional (perlindungan privasi pengguna). Dalam kerangka etika deontologis, tindakan mengabaikan privasi pengguna demi keuntungan bisnis adalah pelanggaran etika yang tidak dapat dibenarkan terlepas dari hasilnya. Sementara itu, dari perspektif konsekuensialis, biaya jangka panjang dari pelanggaran privasi—baik dalam bentuk sanksi hukum, kehilangan kepercayaan publik, maupun kerusakan reputasi—jauh melebihi keuntungan jangka pendek dari mengabaikan privasi.

Wahyudi & Hartono (2025) mengusulkan bahwa profesionalisme TI di era PDP harus dipahami melalui tiga dimensi yang saling terkait: kompetensi teknis (kemampuan mengimplementasikan mekanisme privasi), literasi hukum (pemahaman kewajiban regulasi), dan integritas etika (komitmen terhadap nilai-nilai perlindungan pengguna bahkan tanpa pengawasan eksternal). Ketiga dimensi ini harus diinternalisasi dalam pembentukan identitas profesional praktisi TI, bukan sekadar daftar aturan yang dipatuhi secara mekanis.

4. KESIMPULAN

Berdasarkan analisis mendalam yang telah dipaparkan, penelitian ini menghasilkan tiga kesimpulan utama. Pertama, terdapat korelasi sistematis dan signifikan antara tujuh prinsip fondasi Privacy by Design (PbD) dengan pasal-pasal kewajiban pengendali data dalam UU PDP No. 27 Tahun 2022. Korelasi ini membuktikan bahwa praktisi TI yang mengadopsi PbD secara komprehensif akan secara otomatis memenuhi sebagian besar kewajiban kepatuhan legal yang ditetapkan undang-undang, menjadikan PbD sebagai jembatan efisien antara standar teknis internasional dan regulasi hukum nasional.

Kedua, implementasi PbD di Indonesia menghadapi tiga hambatan struktural yang memerlukan pendekatan multidimensi: keterbatasan literasi regulasi yang membutuhkan reformasi kurikulum pendidikan TI, budaya organisasi berorientasi profit jangka pendek yang perlu diubah melalui pendekatan bisnis berbasis risiko, serta kompleksitas sistem warisan yang menuntut strategi remedisi bertahap dan sistematis. Ketiga tantangan ini tidak dapat diatasi hanya melalui regulasi, melainkan memerlukan transformasi budaya profesional yang mendalam.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1430-1438

Ketiga, kerangka kerja integratif PbD dalam SDLC yang diusulkan dalam penelitian ini memberikan peta jalan praktis bagi pengembang sistem informasi untuk menerjemahkan prinsip-prinsip abstrak PbD menjadi tindakan teknis yang konkret dan terverifikasi di setiap fase pengembangan. Kerangka ini mengisi celah literatur yang selama ini ada antara teori PbD dan implementasi teknis nyata dalam konteks regulasi Indonesia.

Implikasi manajerial dari penelitian ini mengarah pada perlunya organisasi memperkuat tata kelola data melalui pembentukan fungsi Data Protection Officer (DPO), pelaksanaan audit TI berkala, dan pengembangan budaya kepatuhan privasi yang berkelanjutan. Sebagai rekomendasi penelitian lanjutan, kajian empiris berbasis survei dan studi kasus pada sektor-sektor spesifik (seperti fintech, layanan kesehatan digital, dan e-government) diperlukan untuk mengukur tingkat kesiapan aktual implementasi PbD dan mengidentifikasi praktik terbaik yang dapat direplikasi secara nasional.

Pada akhirnya, adopsi Privacy by Design bukan sekadar respons reaktif terhadap tekanan regulasi, melainkan merupakan manifestasi nyata dari profesionalisme dan integritas etis praktisi teknologi informasi dalam melindungi hak asasi fundamental pengguna di era digital. Di tengah akselerasi transformasi digital nasional, menjadikan privasi sebagai nilai inti—bukan sekadar kotak centang kepatuhan—adalah investasi terpenting yang dapat dilakukan Indonesia untuk membangun ekosistem digital yang benar-benar dapat dipercaya.

REFERENCES

Anugrah, S., Himawan, M. Z., Qalby, N. R., & Nurmiati, E. (2025). Pengaruh Etika Profesi Terhadap Keamanan Informasi Dalam Konteks Kebocoran Data Bsi (Bank Syariah Indonesia): Studi Literatur Sistematis. *Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi*, *11*(2), 106-112.

Association for Computing Machinery. (2018). ACM Code of Ethics and Professional Conduct. New York, NY: ACM. https://www.acm.org/code-of-ethics

Beguai, A. (1983). How to Prevent Computer Crime: A Guide for Managers. New York: John Wiley & Sons.

Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Toronto: Information and Privacy Commissioner of Ontario.

European Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.

Ferdiana, R. (2022). Tinjauan Etika dan Privasi dalam Pengembangan Perangkat Lunak di Era Kecerdasan Buatan. Jurnal Sistem Informasi dan Teknologi Informasi, 11(1), 45–58.

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation.

IEEE. (2014). IEEE Code of Ethics. New York: Institute of Electrical and Electronics Engineers.

ISO/IEC 29100:2011. (2011). Information Technology—Security Techniques—Privacy Framework. Geneva: International Organization for Standardization.

Kim, G., Humble, J., Debois, P., & Willis, J. (2019). The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations (2nd ed.). IT Revolution Press.

Lukito, Y. (2023). Komparasi Regulasi Perlindungan Data Pribadi: GDPR Eropa dan UU PDP Indonesia dalam Perspektif Hukum Komparatif. Jurnal Hukum dan Teknologi Informasi, 5(2), 89–112.

Nasution, M. A., & Sari, D. P. (2023). Analisis Kesiapan Praktisi Teknologi Informasi Terhadap Implementasi UU Perlindungan Data Pribadi di Indonesia. Jurnal Riset Informatika dan Inovasi, 1(2), 88–102.

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST. https://doi.org/10.6028/NIST.CSWP.04162018

Nissenbaum, H. (2020). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

Putra, A. S., & Wiguna, A. S. (2021). Implementasi Metode Privacy by Design untuk Meningkatkan Keamanan Data pada Sistem E-Commerce. Jurnal Informatika dan Rekayasa Perangkat Lunak, 3(2), 120–134.

Rahman, R. A., & Nurmiati, E. (2026). Tinjauan Etika Profesi TI pada Standar ACM-IEEE dan SKKNI: Systematic Literature Review. *Sistematis*, *2*(2), 164-172.

Ramadhani, S., & Kurniawan, H. (2024). Tantangan Etika Profesi IT dalam Menghadapi Kebocoran Data Massal: Perspektif Hukum dan Teknis. Jurnal Teknologi Informasi dan Komunikasi, 8(1), 12–25.

Razzaq, R. S. D., & Nurmiati, E. (2026). Tantangan etika dan privasi terhadap cyber crime big data (Studi literatur). *Jurnal Kajian Hukum Dan Kebijakan Publik| E-ISSN: 3031-8882*, *3*(2), 604-608.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

Wahyudi, R., & Hartono, B. (2025). Integrasi Standar ISO/IEC 29100 dan Prinsip Privacy by Design pada Sistem Informasi Publik. Jurnal Ilmiah Teknologi Informasi, 13(3), 210–225.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1430-1438

Waldman, A. E. (2018). Privacy as Trust: Information Privacy for an Information Age. Cambridge University Press.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

Zulkarnain, I. (2023). Dilema Etika dan Tanggung Jawab Profesional Pengembang Sistem dalam Menjaga Kerahasiaan Data Pengguna. Jurnal Etika dan Hukum Teknologi, 2(1), 5–18.