e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Personal Data Protection Law and Information Security Risk Management in Higher Education Institutions

Bimo Satrio Trengginas[1)]
[1)]Study Program of Informatics, Faculty of Technology Industry, Universitas Islam Indonesia
Email: [1)] Bimosatriotrengginas218@gmail.com

How to Cite :
Trengginas. B. S., (2025). Personal Data Protection Law and Information Security Risk Management in Higher Education Institutions . Jurnal Media Computer Science, 4(2). Doi: https://doi.org/10.37676/jmcs.v4i2

ARTICLE HISTORY
Received [25 Juni 2025]
Revised [10 Juli 2025]
Accepted [11 Juli 2025]

KEYWORDS
PDP Law, Risk Management, BPMN, Higher Education Institutions, Information Security.

ABSTRAK

Perkembangan teknologi meningkatkan risiko kebocoran data pribadi, termasuk di lingkungan akademik. Penelitian ini menganalisis penerapan Undang-Undang Pelindungan Data Pribadi (UU PDP) No. 27 Tahun 2022 dalam manajemen risiko pengamanan informasi di institusi pendidikan tinggi. Metode yang digunakan adalah Design Science Research Methodology dengan empat tahap: observasi, wawancara, analisis BPMN, dan evaluasi stakeholder. Hasilnya menunjukkan masih ada kesenjangan antara regulasi dan praktik di lapangan, serta risiko kebocoran data yang signifikan. Model BPMN baru diusulkan untuk meningkatkan kepatuhan dan keamanan data. Evaluasi menunjukkan model ini dapat mendukung institusi pendidikan tinggi dalam mematuhi UU PDP.

ABSTRACT

Technological advancements have increased the risk of personal data breaches, including within academic environments. This research analyzes the implementation of Law No. 27 of 2022 on Personal Data Protection in information security risk management within higher education institutions. The method used is Design Science Research Methodology, comprising four stages: observation, interviews, BPMN annalysis, and stakeholder evaluation. The results indicate a persistent gap between regulation and practical implementation, as well as significant risks of data breaches. A new BPMN model is proposed to enhance compliance and data security. Evaluation demonstrates that this model can support higher education institutions in complying with the PDP Law.

PENDAHULUAN

Di era transformasi digital, teknologi telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari dan dunia pendidikan. Berbagai inovasi teknologi mempermudah aktivitas, namun di sisi lain meningkatkan risiko kejahatan siber, salah satunya adalah kebocoran data pribadi. Laporan Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa pada 2023, Indonesia mengalami lebih dari 300 juta insiden siber, termasuk kebocoran data di berbagai sektor, seperti e-commerce, layanan publik, dan pendidikan tinggi. Universitas sebagai lembaga pendidikan tinggi menyimpan data sensitif mahasiswa, dosen, dan staf yang rentan terhadap serangan. Data-data ini sangat strategis, seperti data akademik, rekam jejak pendidikan, data kepegawaian, dan informasi sensitif lainnya yang jika disalahgunakan dapat menimbulkan kerugian besar baik dari sisi finansial, reputasi, maupun integritas lembaga.

Untuk itu, pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Pemberlakuan Undang-Undang Pelindungan Data

Pribadi (UU PDP) di Indonesia adalah salah satu langkah pencegahan adanya kebocoran data. Langkah ini bisa menjadi *lex specialis* atau hukum yang bersifat khusus dan menjadi langkah awal untuk memahami pelindungan data pribadi di Indonesia (Yuniarti.s 2022). Oleh karea itu, UU PDP menjadi tonggak penting dalam memberikan kepastian hukum dan pelindungan terhadap data pribadi, sejalan dengan tren global seperti General Data Protection Regulation (GDPR) di Eropa. Namun, penerapan UU PDP di sektor pendidikan tinggi menghadapi tantangan besar, mulai dari pemahaman regulasi, keterbatasan infrastruktur, hingga kesenjangan antara kebijakan dan implementasi teknis. Beberapa kampus masih mengalami kendala dalam memetakan alur pemrosesan data, melakukan mitigasi risiko, dann memastikan bahwa data yang dikumpulkan telah mendapatka persetujuan eksplisit dari subjek data. Tantangan lainnya adalah integrasi regulasi internal kampus dengan UU PDP yang baru diterapkan. Pelindungan data pribadi adalah faktor kunci dalam mempertahankan stabilitas sosial serta membangun kepercayaan publik. Ketika data pribadi dijaga dengan baik, masyarakat merasa lebih terlindungi dan aman dari risiko seperti pencurian identitas, penipuan, maupun penyalahgunaan informasi (Pranata et al., 2024).

Penelitian ini bertujuan untuk menganalisis penerapan UU PDP dalam manajemen risiko pengamanan informasi di institusi pendidikan tinggi, menggunakan studi kasus Universitas Islam Indonesia (UII). Penelitian ini juga merancang model proses bisnis baru menggunakan Business Process Model and Notation (BPMN) yang diharapkan dapat mendukung kepatuhan terhadap UU PDP dan meningkatkan ketahanan informasi. Untuk mengeimplementasikan manajemen risiko pada Institusi Pendidikan Tinggi, digunakan BPMN yang bisa menjadi aktivitas kunci agar berjalan efektif dan keselarasan komunikasi yang lebih mudah antara pengguna bisnis seperti Direktorat atau Manajemen Institusi, Sistem, dan Ahli IT yang bertugas merancang dan memelihara sistem informasi Institusi. Melalui BPMN, potensi risiko kebocoran data dapat dipetakan dan dikelola secara efektif, serta dapat memperkuat fondasi pengamanan informasi di seluruh lingkup kerja Institusi Pendidikan Tinggi (Kopp, A. (2022).

LANDASAN TEORI

Asas UU PDP

UU pdp hadir sebagai bentuk pengakuan negara terhadap pentingnya pelindungan data pribadi sebagai hak asasi manusia. Asas yang diatur di dalamnya meliputi kepastian hukum, kemanfaatan, kehati-hatian, dan pertanggungjawaban. Prinsip-prinsip tersebut menjadi landasan untuk memastikan data individu tidak disalahgunakan dan tetap terjaga kerahasiaannya. Asas ini juga menuntut pengendali data untuk mengutamakan prinsip kehati-hatian dan akuntabilitas (Tanzilla et al. 2023).

Risiko kebocoran data

Insiden kebocoran data sering terjadi akibat lemahnya pengamanan dan ketidaksiapan institusi. Contoh kasus kebocoran data di indonesia antara lain peretasan data Tokopedia (2020) yang berdammpak luas. Kebocoran data ini berpotensi merugikan individu dan lembaga, serta memengaruhi kepercayaan publik. Di sektor pendidikan, kebocoran data dapat mencakup data mahasiswa, dosen, serta data akademik yang strategis (Wibowo et al. 2024). Hal ini menjadi ancaman serius bagi kelangsungan operasional lembaga dan integritasnya.

Urgensi manajemen risiko

Manajemen risiko di institusi pendidikan tinggi menjadi kebutuhan mendesak untuk melindungi data sensitif. Penerapan manajemen risiko yang baik dapat meminimalisir potensi kerugian dan meningkatkan tata kelola keamanan informasi. Pendekatan manajemen risiko juga selaras dengan standar internasional seperti ISO 27005 dan NIST yang menekankan pada identifikasi risiko, penilaian, mitigasi, dan monitoring berkelanjutan (Bintarawati. 2024).

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Model BPMN untuk pengamanan data

BPMN adalah alat visualisasi yang efektif untuk memetakan proses bisnis dan mempermudah identifikasi risiko. BPMN membantu memetakan peran setiap aktor, jalur data, dan prosedur keamanan. Implementasi BPMN di sektor pendidikan dapat menjadi landasan untuk merumuskan kebijakan internal yang lebih kuat dan selaras dengan UU PDP (Wong et al. 2022). BPMN mempermudah komunikasi antar stakeholder dan mendukung dokummentasi proses yang transparan.

METODE PENELITIAN

Penelitian ini menggunakan *Design Science Research Methodology* (DSRM) yang dirancang untuk merumuskan solusi terhadap masalah praktis dan ilmiah. Metode ini terdari empat tahap:

1. **Research Clarification:** Studi literatur mendalam untuk memahami kerangka UU PDP dan risiko kebocoran data di institusi pendidikan. Tahap ini bertujuan mengidentifikasi gap antara teori regulasi dan implementasi di lapangan, serta mendokumentasikan kebutuhan yang menjadi latar belakang penelitian.
2. **Descriptive Study I:** Observasi dan wawancara dengan Badan Sistem Informasi UII. Data yang dikumpukan berupa dokumentasi BPMN yang sedang berjalan, kebijakan internal, dan prosedur keamanan yang diterapkan. Analisis data dilakukan dengan pendekatan kualitatif tematik dan pengkodean data untuk mengidentifikasi pola dan kesenjangan.
3. **Prescriptive Study:** Berdasarkan temuan, peneliti merumuskan rancangan model BPMN baru yang memuat elemen-elemen utama UU PDP: persetujuan eksplisit, enkripsi data, prosedur pelaporan kebocoran data, dan penghapusan data tidak diperlukan. Model BPMN dirancang untuk mengoptimalkan pelindungan data dan meningkatkan kepatuhan lembaga.
4. **Descriptive Study II:** Model BPMN usulan divalidasi bersama stakeholder (Badan Sistem Informasi) untuk menilai kesesuaian dengan regulasi dan efektivitasnya. Hasil evaluasi menjadi dasar untuk menyusun kesimpulan dan saran praktis, serta untuk memastikan bahwa model BPMN yang dikembangkan dapat diterapkan secara berkelanjutan di institusi pendidikan tinggi.

HASIL DAN PEMBAHASAN

Hasil

Pada hasil akan menyajikan hasil analisis dan perancangan yang dilakukan dalam penelitian, serta pembahasan mendalam terkait temuan tersebut. Pembahasan akan difokuskan pada analisis kondisi keamanan informasi saat ini di Universitas Islam Indonesia (UII), perancangan model proses bisnis baru yang selaras dengan Undang-Undang Pelindungan Data Pribadi (UU PDP), dan validasi model melalui pengembangan fitur pelaporan insiden.

Pembahasan

Analisis proses bisnis pengamanan informasi saat ini di UII

Berdasarkan hasil observasi dan wawancara yang dilakukan dengan Badan Sistem Informasi (BSI) UII, pemetaan proses bisnis pengamanan data pribadi saat ini berhasil didokumentasikan menggunakan *Business Process Model and Notation* (BPMN). Proses yang berjalan melibatkan lima aktor utama: Pelamar kerja, UII Admisi (Sistem), Admin Unit, Panitia Rekrutmen, dan Direktorat/Manajemen Universitas.

Proses diawali dengan pelamar mengisi data diri melalui sistem UII Admisi. Data tersebut kemudian disimpan oleh sistem dan dapat diduplikasi sebagian oleh Admin Unit untuk keperluan seleksi di tingkat fakultas. Panitia Rekrutmen meninjau dan menyeleksi berkas tersebut, dan hasilnya akan mengubah status lamaran menjadi “lolos” atau “tidak lolos”. Pelamar yang lolos akan melanjutkan ke tahap berikutnya, dan jika berhasil hingga akhir, datanya akan disimpan secara

permanen di *database* dan dapat dikelola oleh Direktorat untuk berbagai keperluan, termasuk otorisasi akses ke pihak eksternal. Dari analisis BPMN saat ini, ditemukan beberapa kesenjangan dan potensi risiko yang tidak selaras dengan prinsip UU PDP, antara lain:

a. Kurangnya Persetujuan Eksplisit: tidak ada mekanisme yang secara eksplisit meminta persetujuan (consent) dari pelamar terkait pengumpulan, pemrosesan, dan penyimpanan data pribadi mereka.
b. Ketidakjelasan Hak Subjek data: proses yang berjalan tidak menyediakan opsi bagi subjek data (pelamar) untuk mengajukan permohonan penghapusan data jika tidak lagi diperlukan.
c. Risiko Keamanan Data: tidak dijelaskan adanya mekanisme enkripsi saat penyimpanan data, sehingga meningkatkan risiko jika terjadi akses tidak sah ke *database.*
d. Manajemen Hak Akses yang Luas: Admin Unit memiliki kemampuan untuk menduplikasi data, yang berpotensi menimbulkan risiko penyebaran data yang tidak terkontrol. Selain itu, tidak ada mekanisme verifikasi berlapis (seperti PIN) saat mengakses data sensitif.
e. Tidak adanya kebijakan retensi dan penghapusan data: Data pelamar yang tidak lolos seleksi tidak dijelaskan proses penghapusannya secara otomatis, sehingga berisiko disimpan melebihi batas waktu yang diperlukan.

Perancangan model BPMN yang diusulkan sesuai UU PDP

Untuk mengatasi kesenjangan yang ditemukan, sebuah odel BPMN baru dirancang dengan mengintegrasikan prinsip-prinsip UU PDP dan manajemen risiko. Model usulan ini menambahkan satu peran baru, yaitu **Superadmin**, dan menyempurnakan alur kerja untuk memastikan kepatuhan dan keamanan.

Berikut adalah fitur-fitur utama dan perbaikan dalam model BPMN yang diusulkan:

a. Manajemen Hak Akses Terpusat: Diperkenalkan peran Superadmin yang bertugas membuat dan mengatur hak akses untuk setiap peran (user) dalam sistem, memastikan bahwa akses terhadap data pribadi diberikan berdasarkan prinsip kebutuhann (need-to-know basis).
b. Mekanisme Persetujuan Eksplisist (Explicit Consent) : Sebelum dapat mengakses sistem, pelamar kerja diwajibkan menyetujui kebijakan privasi yang merujuk pada UU PDP. Jika tidak setuju, akses akan ditolak. Ini memenuhi asas keabsahan pemrosesan data.
c. Implementasi Hak Subjek data: Setelah mengisi data, sistem akan menampilkan pop-up yang memberikan opsi kepada pemilik data untuk mengajukan penghapusan datanya di kemudian hari.
d. Peningkatan Keamanan Teknis:
    1. Enkripsi data: Setiap data yang dikirim dan disimpan oleh sistem akan dienkripsi secara otomatis untuk melindungi kerahasiaan data.
    2. Pencatatan Aktivitas (Logging) : Sistem akan mencatat menampilkan waktu *(created at)* dan *(updated at)* setiap kali ada pembuatan atau pembaruan data, yang berfungsi sebagai jejak audit *(audit trail).*
    3. Verifikasi Berlapis: Admin Unit diwajibkan memasukkan PIN saat akan mengakses data sensitif pelamar, menambahkan lapisan keamanan tambahan.
e. Kebijakan Retensi dan Penghapusan Otomatis: Sistem secara otomatis akan menghapus data pelamar yang dinyatakan tidak lolos seleksi, baik di tahap awal maupun tahap akhir. Hal ini memastikan data tidak disimpan lebih lama dari tujuannya.

Validasi model melalui fitur pelaporan kebocoran data

Sebagai bagian dari evaluasi dan validasi, model yang diusukan diperkuat dengan penambahan fitur Pelaporan Kebocoran Data. Fitur ini dirancang untuk memenuhi kewajiban UU PDP yang mengharuskan pengendali data melaporkan insiden kebocoran data dalam waktu 3x24 jam (72 jam) kepada subjek data dan lembaga terkait.

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Proses pelaporan ini melibatkan tiga aktor: Pelapor, Admin Unit, dan Tim Keamanan Data.

1. Pelapor: (mahasiswa, dosen, staf) dapat mengisi formulir laporan jika menemukan aktivitas mencurigakan pada datanya.
2. Admin Unit: berfungsi sebagai penerima notifikasi awal dan meneruskannnya ke tim terkait.
3. Tim Keamanan Data: bertanggung jawab untuk menganalisis, mengidentifikasi dampak, melalukan mitigasi, dan membuat laporan akhir insiden. Jika data pribadi terbukti terdampak, Admin Unit akan menginformasikan kepada pemilik data yang relevan.

Pembahasan implikasi model yang diusulkan

Perancangan model BPMN baru yang disajikan dalam penelitian ini bukan hanya sekedar perbaikan teknis, melainkan sebuah kerangka straegis bagi institusi pendidikan tinggi untuk mengelola risiko dan mematuhi UU PDP. Temuan ini menunjukkan adanya kesenjangan signifikan antara regulasi yang berlaku dan praktik di lapangan. Model yang ada saat ini cenderung berfokus pada alur kerja administratif tanpa mempertimbangkan aspek risiko keamanan dan hak privasi subjek data secara mendalam.

Model yang diusulkan secara langsung menjawab risiko-risiko utama seperti kebocoran data, penyalahgunaan informasi, dan potensi sanksi hukum. Dengan mengintegrasikan fitur-fitur seperti *consent management,* enkripsi, kebijakan retensi, dan hak akses berjenjang, model ini mengubah pendekatan dari reaktif menjadi proaktif. Institusi tidak lagi hanya merespons insiden, tetap secara sistematis mencegahnya terjadi.

Kehadiran fitur pelaporan insiden juga menjadi krusial. Ini menunjukkan bahwa institusi memiliki mekanisme yang jelas untuk transparansi dan akuntabilitas jika terjadi krisis, yang merupakan kunci untuk mempertahankan kepercayaan publik dan reputasi institusi. Secara praktis, model BPMN ini dapat diadopsi sebagai panduan bagi UII dan institusi pendidikan tinggi lainnya untuk mereformasi tata kelola data pribadi mereka. Implementasinya akan mendorong budaya sadar privasi *(privacy-aware culture)* di lingkungan akademik dan memastikan bahwa inovasi teknologiberjalan seiring dengan pelindungan hak asasi manusia.

KESIMPULAN DAN SARAN

Berdasarkan hasil analisis dan perancangan yang telah diuraikan, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Proses bisnis pengamanan informasi yang berjalan saat ini di Universitas Islam Indonesia (UII), khususnya dalam proses rekrutmen, memiliki kesenjangan signifikan dengan prinsip yang diamanatkan dalam Undang-Undang Pelindungan Data Pribadi (UU PDP). Kesenjangan utama terletak pada tidak adanya mekanisme persetujuan eksplisit (explicit consent), manajemen hak akses yang belum terstruktur, ketidakjelasan kebijakan retensi dan penghapusan data, serta kurangnya lapisan keamanan teknis seperti enkripsi.
2. Model proses bisnis (BPMN) yang diusulkan berhasil mengintegrasikan prinsip-prinsip inti UU PDP untuk memitigasi risiko keamanan data. Dengan memperkenalkan peran Superadmin untuk manajemen akses, mekanisme explicit consent, enkripsi data, pencatatan aktivitas (logging), dan penghapusan data otomatis, model ini menyediakan kerangka kerja yang komprehensif untuk memastikan kepatuhan dan keamanan data pribadi sejak awal proses.
3. Penambahan fitur Pelaporan Kebocoran Data pada model yang diusulkan merupakan komponen krusial yang tidak hanya memenuhi kewajiban pelaporan dalam UU PDP (batas waktu 72 jam), tetapi juga membangun mekanisme respons insiden yang transparan dan akuntabel. Fitur ini memperkuat postur keamanan siber institusi secara keseluruhan.
4. Penelitian ini menghasilkan sebuah artefak berupa model proses bisnis yanng dapat berfungsi sebagai panduan praktis dan strategis bagi institusi pendidikan tinggi di Indonesia untuk mengadaptasi operasional mereka agar selaras dengan regulasi pelindungan data pribadi yang berlaku.

Saran

Berdasarkan kesimpulan yang telah ditarik, berikut adalah beberapa saran yang dapat diajukan:

Saran Implementatif (untuk Institusi) :

1. Universitas Islam Indonesia dan institusi pendidikan tinggi lainnya direkomendasikan untuk mengadopsi dan mengimplementasikan model BPMN yang diusulkan sebagai standar operasional prosedur (SOP) dalam proses rekrutmen dan proses lain yang melibatkan pengelolaan data pribadi.
2. Selain implementasi teknis, institusi perlu menyusun keijakan internal yang mendukung serta melakuak sosialisasi dan pelatihan secara berkala kepada seluruh staf (Admin Unit, Panitia Rekrutmen, dll.) untuk menginngkatkan kesadaran akan pentingnya pelindungan data pribadi dan memastikan model dapat berjalan efektif.

Saran Akademis (untuk penelitian selanjutnya)

1. Cakupan penelitian dapat diperluas untuk menganalisis dan merancang model pengamanan data pada proses bisnis lainnya di universitas yang juga bersifat data-intensif, seperti pengelolaan data akademik mahasiswa, data keuangan, dan data penelitian.
2. Dapat dilakukan studi komparatif di beberapa institusi pendidikan tinggi yang berbeda untuk mendapatkan gambaran yang lebih luas mengenai tingkat kesiapan dan tantangan implementasi UU PDP di sektor pendidikan Indonesia, sehingga dapat dirumuskan rekomendasi yang lebih general.

DAFTAR PUSTAKA

Yuniarti, S. (2022). Protection of Indonesia'S Personal Data After the Ratification of the Draft Personal Data Protection Law. *Progressive In Law*, *4*(2).

Wong, J., Henderson, T., & Ball, K. (2022). Data protection for the common good: Developing a framework for a data protection-focused data commons. *Data & Policy*, *4*, e3.

Bintarawati, F. (2024). THE INFLUENCE OF THE PERSONAL DATA PROTECTION LAW (UU PDP) ON LAW ENFORCEMENT IN THE DIGITAL ERA. *ANAYASA: Journal of Legal Studies*, *1*(2), 135–143.

Wibowo, M. H., & Fatimah, N. (2017). Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime. *JOEICT (Jurnal of Education and Information Communication Technology)*, *1*(1), 1–5.

Tanzilla, F. D., Hanita, M., & Widiawan, B. (2023). Cyber Security In Indonesia Post Establishment Of The Personal Data Protection Law. *International Journal of Progressive Sciences and Technologies (IJPSAT)*, *40*(2).

Kopp, A. (2022). Guidelines and a software tool for quality assessment of BPMN business process models. *Journal of Emerging Technologies*, *2*(2). https://doi.org/10.57040/jet.v2i2.197

Pranata, A., Juono, A. A., & Binarida, A. V. Y. (2024). Implementasi Asas Kehati-Hatian dalam Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi di Era Digital 5.0. *JOURNAL OF LAW AND NATION*, *3*(3), 721–730.