

**MANAJEMEN RISIKO PADA PENGAMANAN INFORMASI
INSTITUSI PENDIDIKAN TINGGI UNTUK IMPLEMENTASI
UU PDP**



Disusun Oleh:

N a m a : Bimo Satrio Trengginas
NIM : 21523233

**PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2025**

HALAMAN PENGESAHAN DOSEN PEMBIMBING

**MANAJEMEN RISIKO PADA PENGAMANAN INFORMASI
INSTITUSI PENDIDIKAN TINGGI UNTUK IMPLEMENTASI
UU PDP**

TUGAS AKHIR



Yogyakarta, 8 Januari 2025

Pembimbing,

(Ari Sujarwo, S.Kom., M.I.T.)

HALAMAN PENGESAHAN DOSEN PENGUJI

MANAJEMEN RISIKO PADA PENGAMANAN INFORMASI INSTITUSI PENDIDIKAN TINGGI UNTUK IMPLEMENTASI UU PDP

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika – Program Sarjana di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 8 Januari 2025

Tim Penguji

Ari Sujarwo, S.Kom., M.I.T.

Anggota 1

Dr. Raden Teduh Dirgahayu, S.T., M.Sc.

Anggota 2

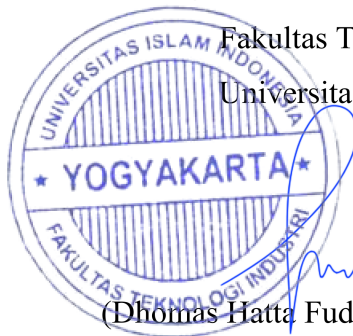
Dr. Feri Wijayanto, S.T., M.T.

Mengetahui,

Ketua Program Studi Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia



(Dhomas Hatta Fudholi, S. T., M.Eng., Ph.D.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Bimo Satrio Trengginas

NIM : 21523233

Tugas akhir dengan judul:

MANAJEMEN RISIKO PADA PENGAMANAN INFORMASI INSTITUSI PENDIDIKAN TINGGI UNTUK IMPLEMENTASI UU PDP

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung risiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 15 Juli 2025



A handwritten signature in black ink, appearing to be "Bimo Satrio Trengginas".

(Bimo Satrio Trengginas)

HALAMAN PERSEMBAHAN

Dengan segala puji syukur kepada Allah SWT dan atas dukungan serta do'a dari orang tercinta, akhirnya Laporan Tugas Akhir ini dapat di selesaikan dengan baik dan tepat waktu. Oleh karena itu, dengan rasa bangga dan bahagia saya ucapkan rasa syukur dan terima kasih kepada:

1. Allah SWT, karena hanya atas izin dan karunia yang diberikan, maka laporan ini dapat di buat dan selesai pada waktunya.
2. Ayahanda Eko Meinarto Hadiangoro dan ibunda Nurul Siti Fatimah yang telah memberikan dukungan moril maupun material serta do'a yang tiada henti untuk kesuksesan saya.
3. Adik saya tercinta Gita Anindya Maheswari yang selalu memberi dukungan, doa, dan semangat untuk menyelesaikan laporan ini.
4. Bapak Ari Sujarwo, S.Kom., M.I.T., selaku dosen pembimbing yang sabar dan teliti telah mengarahkan, memberi masukan, serta berbagi ilmu hingga laporan ini dapat terselesaikan dengan baik.
5. Almamater Universitas Islam Indonesia, seluruh kebanggan bagiku untuk menjadi bagian dari keluarga besar UII. Ilmu dan pengalaman berharga yang kudapatkan di sini telah membentukkan menjadi pribadi yang lebih baik dan siap menghadapi tantangan.
6. Diri saya sendiri, untuk setiap lelah, setiap keraguan dan setiap pengorbanan yang telah ku lalui. Ini adalah bukti bahwa ketekunan akan membuahkan hasil.

HALAMAN MOTO

“Dan aku menyerahkan urusanku kepada Allah”

(Ghafir: 44)

“This too shall pass”

King Solomon

“You can’t change the past, but you can be better in the future.”

Nick

KATA PENGANTAR

Puji syukur kehadiran Tuhan Yang Maha Esa, atas segala rahmat-Nya sehingga saya dapat menyelesaikan tugas akhir berjudul "MANAJEMEN RISIKO PADA PENGAMANAN INFORMASI INSTITUSI PENDIDIKAN TINGGI UNTUK IMPLEMENTASI UU PDP." Laporan ini disusun sebagai salah satu syarat kelulusan pada program studi Informatika di Universitas Islam Indonesia.

Laporan ini bertujuan untuk membahas penerapan UU Pelindungan Data Pribadi serta manajemen risiko dalam pengamanan informasi di institusi pendidikan tinggi. Saya berharap hasil penelitian ini dapat bermanfaat bagi pengembangan keamanan informasi di lingkungan akademik.

Selama penyusunan laporan ini, penulis menghadapi beberapa kendala non-ilmiah, seperti keterbatasan akses data. Namun, berkat bantuan dan dukungan dari berbagai pihak, laporan ini dapat diselesaikan. Terima kasih sebesar-besarnya saya sampaikan kepada dosen pembimbing, keluarga, dan teman-teman yang telah memberikan dukungan dan motivasi.

Saya berharap laporan ini bermanfaat dan menjadi referensi bagi penelitian lebih lanjut. Kritik dan saran yang membangun sangat diharapkan.

Yogyakarta, 15 Juli 2025



(Bimo Satrio Trengginas)

SARI

Laporan Tugas Akhir ini menjelaskan urgensi serta implementasi Undang-Undang Pelindungan Data Pribadi dan manajemen risiko pada pengamanan informasi institusi pendidikan tinggi. Penelitian ini dibuat karena meningkatnya ancaman kejahatan siber, khususnya *phising*, yang menimbulkan risiko serius terhadap kerahasiaan data pribadi para civitas akademika di lingkungan kampus.

Melalui *Design Research Methodology*, penelitian ini dimulai dengan studi literatur untuk memahami konsep dasar Undang-Undang Pelindungan Data Pribadi. Selanjutnya, dilakukan observasi dan wawancara di Universitas Islam Indonesia (UII) untuk memetakan proses bisnis pengamanan informasi yang ada saat ini. Berdasarkan analisis, diusulkan sebuah model proses bisnis baru dalam bentuk diagram BPMN yang telah diselaraskan dengan prinsip-prinsip dan kewajiban Undang-Undang Pelindungan Data Pribadi.

Secara keseluruhan, laporan tugas akhir ini menjelaskan bagaimana penerapan Undang-Undang Pelindungan Data Pribadi yang didukung oleh manajemen risiko yang terstruktur dapat memperkuat keamanan siber dan pelindungan data pribadi di institusi pendidikan tinggi.

Kata kunci: Undang-Undang Pelindungan Data Pribadi (UU PDP), Manajemen Risiko, Keamanan Informasi, Institusi Pendidikan Tinggi, Data Pribadi, Phising, BPMN.

GLOSARIUM

Lex Specialis	Asas hukum yang menyatakan bahwa hukum yang bersifat khusus (spesialis) mengesampingkan hukum yang bersifat umum (generalis) dalam kasus tertentu.
Phising	Suatu bentuk penipuan <i>online</i> dengan mencoba memperoleh informasi sensitif seperti, data pribadi, nama pengguna, dan kata sandi dengan menyamar sebagai entitas terpercaya dalam komunikasi elektronik.
BPMN	Singkatan dari <i>Business Process Model and Notation</i> yaitu sebuah standar grafis untuk proses bisnis yang menyediakan notasi untuk mengidentifikasi langkah-langkah dalam suatu proses.
Cyber Security	Upaya untuk melindungi sistem komputer, jaringan, dan data dari serangan digital.
DRM	Singkatan dari <i>Design Research Methodology</i> yaitu metodologi yang dikembangkan untuk membantu dalam melakukan penelitian secara sistematis.
UU PDP	Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi
Data Pribadi	Informasi mengenai seseorang, baik yang teridentifikasi maupun yang dapat diidentifikasi, baik secara langsung maupun tidak langsung melalui sistem elektronik maupun non-elektronik.

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN DOSEN PEMBIMBING.....	ii
HALAMAN PENGESAHAN DOSEN PENGUJI	iii
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR	iv
HALAMAN PERSEMBAHAN	v
HALAMAN MOTO	vi
KATA PENGANTAR	vii
SARI.....	viii
GLOSARIUM.....	ix
DAFTAR ISI	x
DAFTAR GAMBAR.....	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Metodologi Penelitian	4
1.7 Sistematika Penulisan	4
1.7.1 Bab 1 Pendahuluan.....	4
1.7.2 Kajian Pustaka.....	5
1.7.3 Metodologi Penelitian	5
1.7.4 Hasil dan Pembahasan	5
1.7.5 Kesimpulan dan Saran	5
BAB II KAJIAN PUSTAKA	6
2.1 Kompleksitas Institusi Pendidikan Tinggi Pada Pengamanan Informasi Pribadi..	6
2.2 Peran ISO 27001 dalam Implementasi Prinsip-Prinsip UU PDP	7
2.3 Asas Undang-Undang Pelindungan Data Pribadi	8
2.4 Risiko Kebocoran Data Pada Institusi Pendidikan Tinggi.....	9
2.5 Urgensi Manajemen Risiko Pada Institusi Pendidikan Tinggi	10
2.6 Peran Penting Undang-Undang Pelindungan Data Pribadi.....	11
2.7 Sikap Institusi Pendidikan Tinggi Terkait Undang-Undang Pelindungan Data Pribadi.....	11
BAB III METODE PENELITIAN	13
3.1 Research Clarification.....	14
3.2 Descriptive study I	15
3.3 Prescriptive Study	16
3.4 Descriptive Study II.....	17
BAB IV ANALISIS DAN PEMBAHASAN.....	19
4.1 Analisis Regulasi dan Risiko Dalam Pengamanan Informasi.....	19
4.2 Kondisi Sistem Saat Ini Pada Keamanan Informasi Di UII.....	19
4.3 Perancangan Model BPMN yang Diusulkan	28
4.4 Implementasi Sistem Antarmuka Berdasarkan Model BPMN	31
4.4.1 Persetujuan Eksplisit Ke Pengguna Terhadap Kebijakan Undang-Undang Pelindungan Data Pribadi.....	32
4.4.2 Autentikasi Admin	34
4.4.3 Fitur DPO.....	35

4.4.4	Fitur Pegawai	37
4.5	Evaluasi dan Validasi Model BPMN yang Diusulkan.....	41
	BAB V KESIMPULAN DAN SARAN.....	44
5.1	Kesimpulan	44
5.2	Saran.....	44
	DAFTAR PUSTAKA	46
	LAMPIRAN	49

DAFTAR GAMBAR

Gambar 3. 1 Design Research Methodology	14
Gambar 3. 2 Diagram BPMN dari Sistem UIIADMISI saat ini	16
Gambar 4. 1 Diagram BPMN dari Sistem UIIADMISI saat ini	21
Gambar 4. 2 Halaman Edit Data Diri Pegawai (1)	23
Gambar 4. 3 Halaman Edit Data Diri Pegawai (2)	24
Gambar 4. 4 Halaman Update Data Diri Pegawai (3)	25
Gambar 4. 5 Halaman Update Data Pendidikan Pegawai (4)	26
Gambar 4. 6 Informasi data pribadi di UIIADMISI	27
Gambar 4. 7 Informasi Data Pribadi di UIIADMISI	27
Gambar 4. 8 Diagram BPMN yang di propose untuk UIIADMISI	29
Gambar 4. 9 Persetujuan eksplisit ke pengguna (1)	32
Gambar 4. 10 Persetujuan eksplisit ke pengguna (2)	33
Gambar 4. 11 Persetujuan eksplisit ke pengguna (3)	33
Gambar 4. 12 Persetujuan eksplisit ke pengguna (4)	34
Gambar 4. 13 Persetujuan Eksplisit ke pengguna (5)	34
Gambar 4. 14 Autentikasi Admin Unit	35
Gambar 4. 15 Dashboard DPO (1)	37
Gambar 4. 16 Dashboard DPO (2)	36
Gambar 4. 17 Laporan dan Analitik	37
Gambar 4. 18 Dashboard Pegawai Lolos Seleksi	38
Gambar 4. 19 Dashboard Pegawai Tidak Lolos Seleksi	38
Gambar 4. 20 Pusat Privasi (1)	39
Gambar 4. 21 Pusat Privasi (2)	39
Gambar 4. 22 Pop-up Pembaruan Data	40
Gambar 4. 23 Data Pribadi Pengguna	41
Gambar 4. 24 Diagram BPMN Pelaporan Kebocoran Data	42
Gambar 4. 25 Lapor Insiden	43

BAB I PENDAHULUAN

1.1 Latar Belakang

Hasil kreativitas dan pemikiran manusia yang dirancang untuk mempermudah kehidupan adalah teknologi. Melalui teknologi, berbagai alat dan sistem diciptakan untuk meningkatkan efisiensi serta menyederhanakan aktivitas sehari-hari, seperti komunikasi dan transportasi (Sulistianingsih et al., 2023). Dengan demikian, semakin pesatnya perkembangan teknologi, banyak inovasi baru yang bermunculan. Namun, seiring dengan kemajuan ini terdapat beberapa dampak negatif salah satunya adalah kejahatan di dunia maya yang dikenal sebagai kejahatan siber. Contoh yang sering terjadi dalam beberapa tahun terakhir adalah peretasan data. Kejahatan ini menghadirkan ancaman serius terhadap keamanan siber, terutama dalam hal perlindungan data pribadi. Data yang dahulu disimpan secara konvensional kini mengalami perubahan besar. Perubahan ini membuat perlindungan data menjadi lebih kompleks, karena adanya potensi kerentanan terhadap serangan siber yang terus berkembang sejalan dengan kemajuan teknologi (Arthaputri, 2024).

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). Kepercayaan ini memiliki peran krusial dalam membentuk hubungan yang baik antara warga negara dan berbagai institusi, termasuk pemerintah maupun sektor swasta. Penyalahgunaan data pribadi bisa menimbulkan kerugian besar bagi individu dan masyarakat luas. Oleh karena itu, dengan adanya perlindungan data yang kuat, potensi penyalahgunaan dapat dikurangi. Ini tidak hanya melindungi individu dari kerugian pribadi, tetapi juga membantu mencegah kejahatan siber yang dapat mengancam stabilitas sosial dan ekonomi negara (Pranata et al., 2024). Oleh karena itu, perlindungan data pribadi sangatlah penting di era digital saat ini. Informasi pribadi seperti nama, nomor identitas, alamat, nomor telepon, dan sebagainya adalah bagian tak terpisahkan dari identitas individu. Para pelaku kejahatan siber sering memanfaatkan data pribadi ini melalui metode *phishing*, yaitu tindakan kriminal yang bertujuan untuk mendapatkan informasi rahasia dari korban secara ilegal (M. H. Wibowo & Fatimah, 2017). *Phishing* adalah upaya untuk mengakses data seseorang melalui teknik penipuan. Data yang diincar dalam serangan *phishing* meliputi

informasi pribadi (seperti nama, usia, alamat), data akun (*username* dan *password*), serta data finansial (informasi kartu kredit atau rekening bank. Pelaku *phishing* sering disebut sebagai *Phisher*, seringkali menyamar sebagai entitas yang sah atau terpercaya dalam komunikasi elektronik, seperti bank, perusahaan, atau situs web terkenal (Sutarli & Kurniawan, 2023). *Phisher* menggunakan berbagai cara untuk meyakinkan korban agar mau membagikan informasi pribadi mereka, misalnya dengan mengirimkan email palsu atau membuat situs web tiruan yang tampak hampir identik dengan yang asli (Sutarli & Kurniawan, 2023).

Indonesia sebagai negara hukum telah berupaya mengatasi masalah terkait data pribadi dengan menetapkan dan/atau mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU PDP ini mengatur berbagai hal yang dapat diimplementasikan pada institusi pendidikan tinggi, seperti pada pasal 3 UU PDP yang menjelaskan asas dari Undang-Undang Pelindungan Data Pribadi, lalu pada pasal 4 UU PDP menjelaskan jenis data pribadi, selanjutnya pada pasal 5 sampai pada pasal 15 menjelaskan hak-hak subjek data pribadi, kemudian pada pasal 16 sampai pada pasal 18 menjelaskan rangkaian pemrosesan data pribadi, serta pada pasal 19 sampai pada pasal 54 menjelaskan hak pengendali data pribadi dan prosesor data pribadi secara sembarangan. Lalu, di dalam Undang-Undang Pelindungan Data Pribadi terdapat beberapa pasal yang tidak relevan terkait pengamanan informasi data pribadi pada institusi pendidikan tinggi, seperti pada Pasal 62 ayat 1 Undang-Undang Pelindungan Data Pribadi yang berbunyi “Kerja sama internasional dilakukan oleh Pemerintah dengan pemerintah negara lain atau Organisasi Internasional terkait dengan Pelindungan Data Pribadi” yang menjelaskan bagaimana ranah Pemerintah melakukan kerja sama dengan pemerintah lain atau Organisasi internasional. Oleh karena itu, pasal tersebut tidak relevan dengan pengamanan informasi pada institusi pendidikan tinggi.

Dengan adanya Undang-Undang Pelindungan Data Pribadi dapat menjadi langkah-langkah yang tepat untuk menjadi landasan hukum yang kuat dan dapat meminimalisirkan risiko yang akan timbul kepada institusi pendidikan tinggi, seperti kebocoran data pribadi para civitas akademika, lalu adanya indikasi akses tidak sah dalam pemrosesan data pribadi, dan sistem pengelolaan data di beberapa kampus masih bersifat desentralisasi, di mana setiap unit (fakultas, departemen, administrasi) memiliki prosedur tersendiri. Kondisi ini berpotensi menciptakan kerentanan dalam pengamanan informasi data pribadi (Fachri Yamin Universitas Janabadra Yogyakarta et al., 2024)

Fokus pada penelitian ini menjelaskan bagaimana institusi pendidikan tinggi seperti Universitas Islam Indonesia (UII) dapat menyelaraskan proses operasionalnya. Seperti contoh

proses alur rekrutmen pegawai pada UIIADMISI yang dapat diselaraskan dengan prinsip-prinsip Undang-Undang Pelindungan Data Pribadi (UU PDP). Dalam proses rekrutmen pegawai memiliki beberapa titik yang menjadi hal kritis dalam manajemen risiko pengamanan data, sedangkan berbeda dengan sistem yang sudah stabil seperti UIIAkademik dan UIIInsani yang sudah terdapat di dalam sistem UIIGateway. Proses alur rekrutmen pegawai merupakan gerbang utama masuknya data pribadi dari pihak eksternal yang belum terverifikasi secara penuh sebagai bagian dari institusi. Proses ini memiliki titik yang sangat rentan terhadap serangan siber dari luar seperti *phishing* dan tidak adanya transparansi ketika pertukaran data sehingga dapat berpotensi adanya indikasi akses secara tidak sah dalam rangkaian pemrosesan data pribadi. Oleh karena itu, proses alur rekrutmen pegawai dapat disesuaikan dengan prinsip-prinsip UU PDP untuk mengamankan proses-proses pengamanan informasi data pribadi.

1.2 Rumusan Masalah

1. Bagaimana penerapan Undang-Undang Pelindungan Data Pribadi (UU PDP) dalam manajemen risiko pengamanan informasi di institusi pendidikan tinggi?
2. Apa saja risiko yang dihadapi oleh institusi pendidikan tinggi jika tidak adanya manajemen risiko untuk melindungi data pribadi sesuai dengan UU PDP?

1.3 Batasan Masalah

1. Penelitian ini hanya membahas aspek keamanan informasi terhadap data personal, seperti data mahasiswa, dosen, dan tenaga pendidikan lainnya, tanpa mencakup data lainnya yang bersifat finansial atau bisnis organisasi lainnya.
2. Penelitian ini hanya berfokus pada proses alur rekrutmen pegawai di UIIADMISI pada Universitas Islam Indonesia untuk memberikan gambaran jika UU PDP diselaraskan dan diterapkan pada institusi pendidikan tinggi di Indonesia.
3. Penelitian ini hanya berfokus pada institusi pendidikan tinggi, seperti universitas atau institut, tanpa mencakup sekolah menengah atau lembaga pendidikan nonformal lainnya.
4. Penelitian ini hanya merekomendasikan penerapan UU PDP kepada pihak kampus untuk keamanan informasi pribadi seperti data mahasiswa, data dosen, dan tenaga kependidikan lainnya dalam rangka peningkatan pengamanan, data berdasarkan landasan hukum.
5. Penelitian ini menggunakan pendekatan *Business Process Model and Notation* (BPMN) untuk memetakan proses pengamanan data pribadi saat ini dan desain proses baru yang telah disesuaikan dengan UU PDP.

1.4 Tujuan Penelitian

1. Menganalisis bagaimana UU PDP diterapkan dalam manajemen risiko yang berkaitan dengan pengamanan data pribadi di institusi pendidikan tinggi.
2. Mengidentifikasi tantangan serta risiko yang dihadapi institusi pendidikan tinggi dalam mengelola pengamanan data pribadi dan mencari solusi untuk mengurangi risiko tersebut.

1.5 Manfaat Penelitian

1. Manfaat Teoritis: Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan ilmu pengetahuan di bidang manajemen risiko dan perlindungan data pribadi, khususnya dalam konteks institusi pendidikan tinggi
2. Manfaat Praktis: Penelitian ini dapat menjadi panduan bagi institusi pendidikan tinggi dalam mengimplementasikan manajemen risiko terkait pengamanan informasi sesuai dengan ketentuan UU PDP.
3. Manfaat Kebijakan: Penelitian ini dapat memberikan masukan bagi para pembuat kebijakan di sektor pendidikan untuk memperbaiki regulasi dan kebijakan terkait pengelolaan risiko pengamanan informasi.

1.6 Metodologi Penelitian

Penelitian ini menggunakan *Design Research Methodology* untuk menganalisis hingga merancang solusi yang relevan dengan konteks Manajemen Risiko pada Pengamanan Informasi Institusi Pendidikan Tinggi untuk Implementasi UU PDP. Metode ini diawali dengan menganalisis data melalui dua pendekatan yaitu observasi dan wawancara terhadap Badan Sistem Informasi agar mendapatkan BPMN yang saat ini digunakan untuk dijadikan bahan pertimbangan dengan BPMN yang selanjutnya dalam membantu dan mendukung UU PDP terkait Pelindungan Data Diri di institusi tinggi seperti UIN.

1.7 Sistematika Penulisan

Sistematika penulisan laporan akhir ini adalah sebagai berikut :

1.7.1 Bab 1 Pendahuluan

Berisi latar belakang yang berisi kondisi yang melatarbelakangi penelitian, selanjutnya rumusan masalah yang menjadi dasar bagi penetapan tujuan penelitian. Lalu disertakan batasan masalah yang menjelaskan ruang lingkup dan keterbatasan penelitian untuk memastikan fokus tetap pada aspek aspek yang relevan. Serta terdapat tujuan dan manfaat penelitian yang diharapkan berkontribusi baik secara teoritis maupun praktis.

1.7.2 Kajian Pustaka

Kajian pustaka merupakan bagian yang menjelaskan tinjauan penelitian sebelumnya, dan konsep-konsep relevan untuk mendukung penelitian. Bagian ini bertujuan menyediakan dasar ilmiah, mengidentifikasi kesenjangan pengetahuan, dan menunjukkan kontribusi penelitian. Selain itu, kajian pustaka membantu merumuskan masalah, tujuan, serta mendukung pemilihan metode penelitian yang tepat.

1.7.3 Metodologi Penelitian

Berisi berbagai tahapan dan kebutuhan penelitian sebagai acuan untuk mencapai solusi atas permasalahan dalam penelitian ini. Bab ini terdiri dari pengumpulan data, pra-pengolahan data, pengolahan data, dan analisis data.

1.7.4 Hasil dan Pembahasan

Berisi hasil dan pembahasan dari setiap proses. Proses pengujian data mahasiswa sampai dengan hasil yang diinginkan. Serta validasi untuk membuktikan keakuratan hasil.

1.7.5 Kesimpulan dan Saran

Berisi kesimpulan mengenai hasil penelitian yang telah sesuai dengan tujuan penelitian atau belum serta saran yang mendukung agar penelitian ini dapat dilanjutkan oleh para peneliti lain dengan mengembangkan keterbatasan dan kekurangan yang terdapat pada penelitian ini.

BAB II

KAJIAN PUSTAKA

2.1 Kompleksitas Institusi Pendidikan Tinggi Pada Pengamanan Informasi Pribadi

Kondisi saat ini di sistem institusi pendidikan tinggi global menunjukkan bahwa harus dilakukan evaluasi terhadap krisis yang tengah berlangsung dengan pemantauan kondisi terkini dan prospek masa depan dalam bidang yang meliputi pendidikan modern, ilmu pengetahuan, dan inovasi yang sangat cepat menunjukkan harus dilakukan adanya transformasi pada struktur kepemimpinan dan manajemen di perguruan tinggi (Ridei et al., 2021). Organisasi Internasional Standarisasi (ISO) dan Komisi Elektroteknik Internasional (IEC) (ISO/IEC 27001); serta *Control for Information and Related Technologies* (COBIT) menjelaskan bahwa saat ini tidak ada satu pun institusi pendidikan tinggi yang mengembangkan kerangka kerja terkait bagaimana keamanan informasi yang melibatkan cara untuk menangani pelanggaran keamanan. Desentralisasi adalah jaringan yang saat ini digunakan oleh sebagian besar institusi pendidikan tinggi sebagai sumber daya komputasi yang terdistribusi. Desentralisasi digunakan juga oleh institusi pendidikan tinggi sebagai proses transfer informasi dan berpotensi rentan. Oleh karena itu, institusi pendidikan tinggi membutuhkan kerangka keamanan dalam pengamanan informasi untuk memastikan kepatuhan terhadap kebijakan regulasi yang berlaku saat ini terkait keamanan dan perlindungan sumber daya vital (Hina & Dominic, 2020).

Institusi pendidikan tinggi memiliki kewajiban untuk melakukan migrasi data pribadi dosen, tenaga pendidikan, dan mahasiswa aktif ke Pangkalan Data Pendidikan Tinggi (PDDIKTI, Kemendikbudristek) terutama ketika terjadi perubahan entitas institusi atau program studi. Proses ini dimulai dengan serangkaian persiapan yang ketat di tingkat internal institusi pendidikan tinggi sesuai regulasi yang diikuti oleh PDDIKTI berdasarkan Undang-Undang Republik Indonesia Nomor 12 Tahun 2012 tentang Pendidikan Tinggi yang dijadikan sebagai alat hukum untuk mewajibkan adanya PDDIKTI dan kewajiban pelaporan data oleh institusi pendidikan tinggi. Kemudian Permenristekdikti Nomor 31 Tahun 2022 tentang Satu

Data Pendidikan dan Permenristekdikti Nomor 61 Tahun 2016 memberikan kerangka kerja yang cukup detail tentang bagaimana PDDIKTI mengelola data tersebut, serta terdapat Surat Edaran Kepala Pusdatin yang mengatur prosedur spesifik untuk kasus migrasi data.

Berdasarkan buku yang diterbitkan oleh PDDIKTI yaitu Buku Saku Migrasi Data PDDikti Tahun 2022 dijelaskan proses yang cukup kompleks terkait migrasi data, meliputi *Cut Off* pelaporan yang dilakukan berdasarkan tanggal Surat Keputusan (SK) perubahan entitas, kemudian Cek Ajuan untuk memastikan tidak ada draf ajuan perubahan data mahasiswa, dosen, dan registrasi dosen, dilanjutkan dengan *Fill Out* Pelaporan untuk memastikan tidak ada data yang salah maupun tertinggal, serta *Over* Pelaporan untuk menghapus seluruh pelaporan yang melebihi batas *Cut Off*. Selain itu, terdapat Masa Tenggang yang mengharuskan institusi pendidikan tinggi tidak meluluskan atau menerbitkan ijazah sampai dengan penyesuaian akreditasi di BAN-PT selesai, dan terakhir adalah persiapan Berkas Persyaratan wajib seperti Surat Ajuan Migrasi Data PDDikti, Surat Pernyataan Selesai Pelaporan, *Checkpoint* Pelaporan PDDikti, serta Surat Permohonan akun institusi pendidikan tinggi. Setelah seluruh persiapan dan kelengkapan berkas terpenuhi, setiap institusi pendidikan tinggi kemudian mengajukan permohonan migrasi data ke LLDikti Wilayah III melalui aplikasi SILAT, yang akan dilanjutkan dengan proses verifikasi dan validasi berkas oleh pegawai LLDikti. Apabila seluruh berkas telah sesuai, perguruan tinggi dapat mengajukan migrasi data melalui laman PDDikti-Admin untuk waktu 3 bulan sejak SK diterbitkan. Pasca-migrasi, perguruan tinggi memiliki tanggung jawab final untuk mencocokkan hasil data migrasi dengan data terakhir sebelum migrasi, serta melakukan instalasi *Feeder*, *generate prefill*, dan sinkronisasi data untuk memastikan integritas dan informasi akurat yang termigrasi ke PDDikti.

2.2 Peran ISO 27001 dalam Implementasi Prinsip-Prinsip UU PDP

Organisasi Standarisasi Internasional (ISO) 27001 mendefinisikan Information Security Management System (ISMS) sebagai kerangka kerja untuk menangani risiko terhadap pengamanan informasi yang lebih efektif. Kerangka kerja ini berlaku untuk organisasi dari berbagai ukuran dan sektor, agar dapat memastikan adaptasi terhadap langkah-langkah keamanan dalam pengamanan informasi terhadap ancaman yang terus berkembang. ISO 27001 tidak hanya menetapkan kontrol khusus tetapi mengacu terhadap fleksibilitas keamanan informasi. Fleksibilitas ini memungkinkan organisasi untuk memilih kontrol berdasarkan penilaian risiko dengan menekankan pendekatan manajemen risiko yang komprehensif (Amine et al., 2023) .

Mengingat kompleksitas keamanan informasi institusi pendidikan tinggi di lingkungan akademik, adanya ISO 27001 adalah hal yang sangat krusial dan sangat penting (Disterer, 2013). Indonesia telah mengesahkan Undang-Undang No 27 Tahun 2022 Tentang Pelindungan Data Pribadi yang mengadopsi ISO 27001 dapat menjadi landasan hukum yang kuat dalam keamanan data pribadi di Indonesia. ISO 27001 menyediakan pendekatan sistematis untuk mengelola informasi sensitif, memastikan kerahasiaan, integritas, dan ketersediaannya (Primaranti et al., 2023) Oleh karena itu, ISO 27001 memiliki standar untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi yang dapat diimplementasikan pada institusi pendidikan tinggi yang dapat menjadi alat untuk menganalisis dan mengatasi tantangan keamanan informasi yang dihadapi oleh perguruan tinggi.

2.3 Asas Undang-Undang Pelindungan Data Pribadi

Undang-Undang Pelindungan Data Pribadi merupakan amanat dari pasal 28G ayat (1) Undang-Undang Dasar Republik Indonesia yang berbunyi “Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.”

Adanya kebocoran data yang kerap terjadi membuat pemerintah harus memilih tindakan tegas. Hal ini juga dipengaruhi oleh kejadian yang beberapa tahun belakangan ini sangat merugikan masyarakat Indonesia. Seperti pada tahun 2020 Indonesia mengalami kebocoran 1,3 miliar data pelanggan kartu SIM, dan di tahun yang sama platform e-commerce Tokopedia juga mengalami peretasan data sebanyak 15 juta akun yang dipublikasikan di Raid Forum. Bahkan pada bulan September 2022, Kementerian Komunikasi dan Informatika mengalami kebocoran data yang diretas oleh akun yang bernama BJORKA (Shahrullah et al., 2024).

Ketika kasus kebocoran data pada Tokopedia terjadi, Indonesia hanya mempunyai Undang-Undang Nomor 1 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang mengatur perkara informasi transaksi elektronik secara umum. Hal ini menunjukkan bahwa Indonesia belum mempunyai Undang-Undang yang secara khusus mengatur pelindungan data pribadi. Sebab itu konsumen dan pengguna tidak memiliki pelindungan hukum ketika mengalami insiden kebocoran data sehingga berdampak pada penurunan kepercayaan terhadap keamanan aplikasi tersebut (A. Wibowo et al., 2024).

Pemerintah telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi pada bulan Oktober 2022 dengan masa transisi 2 tahun. Pada bulan

oktober 2024 lalu Undang-Undang tersebut mulai diberlakukan. Sebelum UU PDP dibuat, Indonesia memiliki Undang-Undang Nomor 1 Tahun 2016 tentang Informasi dan Transaksi Elektronik tetapi tidak menjelaskan mengenai mekanisme perlindungan data pribadi dan hak-hak masyarakat dalam mengolah dan mengendalikan data pribadi mereka. Diharapkan adanya regulasi dari pemerintah dapat menjamin kepastian hukum bagi masyarakat Indonesia yang sering menjadi korban kebocoran data (Simbolon & Juwono, 2022).

Undang-Undang Pelindungan Data Pribadi (UU PDP) No. 27 Tahun 2022 mengatur beberapa hal terkait perlindungan data pribadi di Indonesia yang mengacu pada keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi. UU PDP berlandaskan pada asas perlindungan, kepastian hukum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan. Hak dan kewajiban yang diatur dalam Undang-Undang menjamin hak-hak subjek data pribadi, seperti hak mengetahui, hak untuk memperbaiki, dan hak untuk menghapus data pribadi serta kewajiban pengendali data pribadi untuk melindungi dan memberitahu subjek data pribadi tentang pemrosesan data pribadi.

2.4 Risiko Kebocoran Data Pada Institusi Pendidikan Tinggi

Pada bulan Juli 2024, Universitas Teknologi Muhammadiyah Jakarta mengalami insiden serangan *ransomware* yang menyebabkan pencurian data Personal Data Nasional (PDN). Rektor UTMJ mengonfirmasi insiden tersebut dan menyatakan keprihatinan dan akan meningkatkan keamanan siber. Insiden ini menjelaskan betapa pentingnya keamanan data di institusi pendidikan. Universitas harus memiliki beberapa lapisan cadangan dari data pribadi para civitas akademika untuk meminimalisir risiko yang terjadi dalam pengamanan informasi di institusi pendidikan tinggi.

Undang-Undang Nomor 27 Tahun 2022 tentang Undang-Undang Pelindungan Data Pribadi terdiri dari 76 pasal yang menjadikan itu sebagai jaminan data penduduk Indonesia agar keamanan data mereka terorganisir dan menghindarkan penggunaan data di luar kendali oleh pihak yang tidak bertanggung jawab. Hal ini di dukung oleh isi dari Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang menyebutkan bahwa “Pelindungan data pribadi adalah bagian dari hak asasi manusia yang terkait dengan perlindungan diri, sehingga diperlukan dasar hukum menjamin keamanan data pribadi sesuai dengan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.” (Tanzilla et al., 2023).

Hingga saat ini, kebocoran dan perdagangan data pribadi yang dilakukan secara ilegal menjadi perhatian masyarakat Indonesia karena berkaitan dengan keamanan data pribadi mereka. Upaya pemerintah dalam menangani hal ini cukup lamban, sehingga masyarakat merasa tidak aman dengan adanya kebocoran data yang terjadi setiap tahun di Indonesia. Pemerintah harus lebih siap dengan tantangan yang lebih kompleks, karena seiring berjalannya waktu kemajuan teknologi terus berkembang pesat. Oleh karena itu masyarakat mendesak pemerintah agar memulai perubahan terkait Pelindungan Data Pribadi. Hal ini juga dapat menjadi dampak serius kepada masyarakat, karena khususnya Generasi Y yang sudah banyak untuk memilih tutup mata mengenai kemajuan teknologi yang berkembang cukup pesat (Bintarawati, 2024).

2.5 Urgensi Manajemen Risiko Pada Institusi Pendidikan Tinggi

Pangkalan Data Pendidikan Tinggi, adalah basis data atau sistem yang menghimpun seluruh data pendidikan tinggi dari seluruh perguruan tinggi yang terintegrasi secara nasional yang biasa dikenal dengan PDDikti. Seluruh informasi dan data pendidikan tinggi sudah diolah untuk tujuan tertentu. Sedangkan unit atau tim yang bertanggung jawab dan berhak mengelola serta mengoordinasikan seluruh proses Sertifikasi Dosen di setiap perguruan tinggi disebut Panitia Sertifikasi Dosen pada Perguruan Tinggi Pengusul yang memiliki singkatan PSD-PTU.

PDDikti dan PSD-PTU memiliki pengaturan yang cukup ketat untuk melindungi data rahasia para civitas akademika di Perguruan Tinggi Negeri dan Swasta. Adanya pengaturan tersebut untuk menjamin bahwa data pribadi yang dimiliki civitas akademika memiliki perlindungan di hadapan hukum (Junaedi et al., 2023). Universitas harus memiliki beberapa lapisan cadangan dari data pribadi para civitas akademika untuk meminimalisir risiko yang terjadi dalam pengamanan informasi di institusi pendidikan tinggi. Oleh karena itu, cadangan tersebut dapat dibuat dengan cara klasifikasi data melalui pengembangan yang dilakukan oleh pihak institusi. Hal ini merupakan tindakan efektif yang diperlukan oleh institusi, karena semakin banyak cadangan tersebut akan membuat risiko lebih kecil dan penanganan yang cukup efisien jika terjadi kebocoran data atau adanya penggunaan data yang dilakukan oleh pihak tidak bertanggung jawab (Wong et al., 2022).

Untuk mengimplementasikan manajemen risiko pada institusi pendidikan tinggi, digunakan *Business Process Model and Notation* (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, 2022).

2.6 Peran Penting Undang-Undang Pelindungan Data Pribadi

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, 2022).

Pada pasal 3 Undang-Undang Nomor 27 Tahun 2022 tentang Undang-Undang Pelindungan Data Pribadi yang berbunyi “Undang-Undang ini berasaskan: pelindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan.” menegaskan bahwa Undang-Undang ini bertujuan untuk memberikan pelindungan hukum yang kuat terhadap hak setiap orang terkait data pribadi mereka, baik di dalam maupun di luar Indonesia, termasuk pemrosesan Data Pribadi yang dilakukan oleh institusi Pendidikan.

Dengan adanya Undang-Undang Nomor 27 Tahun 2022 tentang Undang-Undang Pelindungan Data Pribadi dapat menjadi fondasi untuk menjaga kepercayaan civitas akademika dan reputasi lembaga karena dijelaskan bagaimana proses pengelolaan data pribadi serta menegaskan hak-hak subjek data pribadi, antara lain mengelola data pribadi yang sangat besar dan sensitif dari para civitas akademika termasuk mahasiswa, tenaga pendidikan, dan dosen.

2.7 Sikap Institusi Pendidikan Tinggi Terkait Undang-Undang Pelindungan Data Pribadi

Dengan adanya Undang-Undang Nomor 27 Tahun 2022 tentang Undang-Undang Pelindungan Data Pribadi dapat membuat suatu keputusan kepada institusi pendidikan negeri maupun Swasta untuk membuat suatu regulasi terkait Pelindungan Data Pribadi antara para Pegawai, Admin, Mahasiswa, dan Dosen, baik di institusi Pendidikan Tinggi Negeri maupun Swasta, yang akan menjadi salah satu bentuk jaminan pelindungan atas kepastian hukum yang adil (Junaedi et al., 2023).

Berdasarkan Pasal 19 Undang-Undang Pelindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022 yang berbunyi “Pengendali Data Pribadi dan Prosesor Data Pribadi meliputi: Setiap orang, Badan Publik, Organisasi Internasional.”. Oleh karena itu, Pengendali Data

Pribadi diartikan sebagai setiap orang, badan publik dan organisasi internasional yang memiliki hak untuk menentukan tujuan serta dapat melakukan kendali penuh pemrosesan data pribadi. Oleh karena itu, institusi pendidikan tinggi secara jelas memenuhi kriteria untuk mengendalikan pemrosesan data pribadi seluruh civitas akademika termasuk, mahasiswa, dosen, dan tenaga pendidikan. Sebagai pengendali data pribadi, institusi pendidikan tinggi sistem memiliki kewajiban yang harus diikuti berdasarkan Undang-Undang, antara lain memperoleh persetujuan yang sah dari subjek data pribadi, melakukan pemrosesan data sesuai tujuan yang disepakati, menjaga kerahasiaan dan keamanan data, serta memberitahukan adanya indikasi pelanggaran data pribadi kepada Subjek Data dan Lembaga Pelindungan Data Pribadi seperti yang dijelaskan pada Pasal 46 ayat 1 yang berbunyi “Dalam hal terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 jam kepada: Subjek Data pribadi dan lembaga.”.

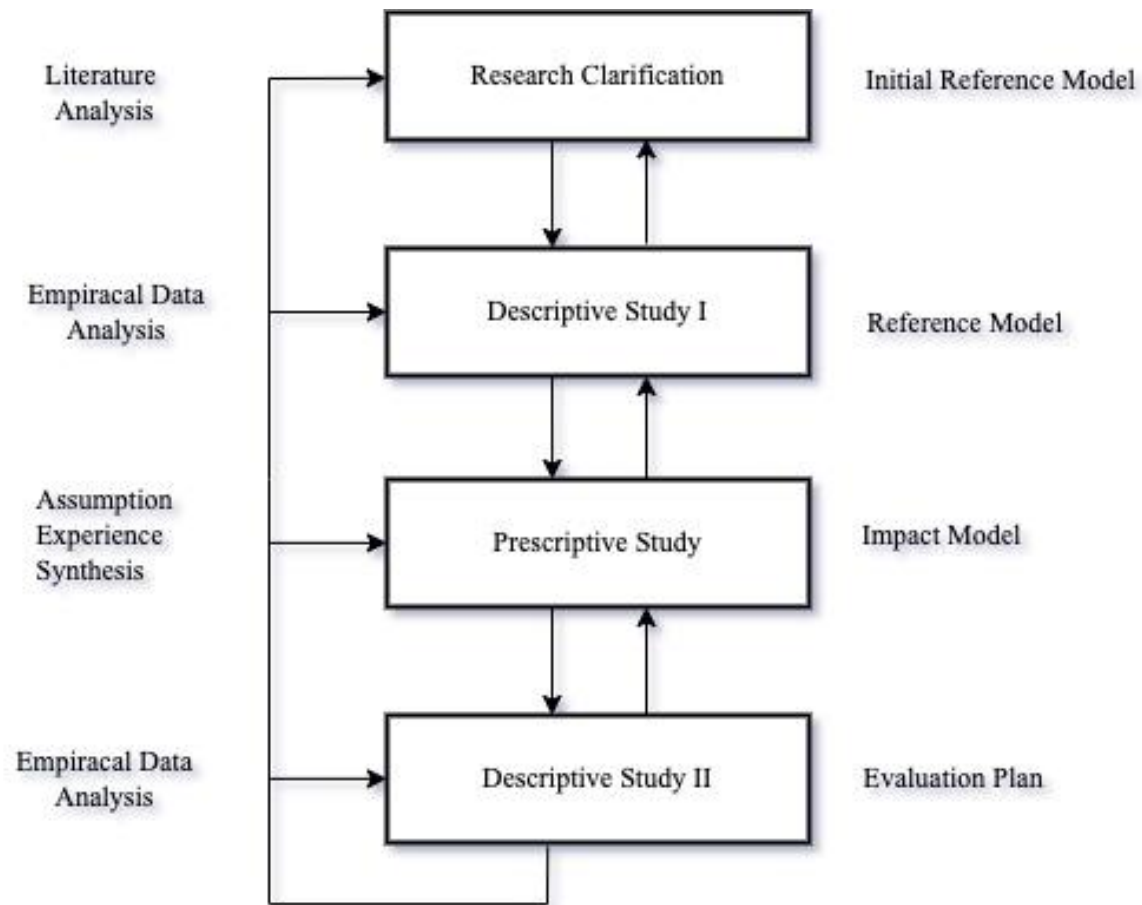
BAB III

METODE PENELITIAN

Penelitian ini menggunakan *Design Research Methodology* untuk menganalisis hingga merancang solusi yang relevan dengan konteks Manajemen Risiko pada Pengamanan Informasi Institusi Pendidikan Tinggi untuk Implementasi UU PDP. Metode ini mencakup beberapa tahap, yaitu *Research Clarification*, *Descriptive Study I*, *Prescriptive Study*, dan *Descriptive Study II*. Metode ini diawali dengan menganalisis data melalui dua pendekatan yaitu *Research Clarification* dan *Descriptive Study I* yang dilakukan melalui observasi dan wawancara terhadap Badan Sistem Informasi.

Hasil observasi dan wawancara yang telah dilakukan menghasilkan pemetaan proses bisnis yang saat ini diterapkan, yang kemudian divisualisasikan dalam bentuk diagram *Business Process Model and Notation* (BPMN). Proses bisnis tersebut selanjutnya dianalisis dengan merujuk pada prinsip-prinsip yang tertuang dalam Undang-Undang Pelindungan Data Pribadi (UU PDP) serta pendekatan manajemen risiko.

Berdasarkan hasil analisis tersebut, disusun rancangan proses bisnis baru untuk proses alur rekrutmen di dalam sistem UIIADMISI yang terdapat di Universitas Islam Indonesia yang diharapkan dapat diimplementasikan secara efektif dan sesuai dengan ketentuan UU PDP, sebagai bagian dari upaya sistematis untuk meningkatkan pelindungan data pribadi dalam sistem informasi di lingkungan institusi pendidikan tinggi, seperti Universitas Islam Indonesia (UII).



Gambar 3. 1 Design Research Methodology

3.1 Research Clarification

Tahap *research clarification* dilakukan untuk mencari bukti atau indikasi yang mendukung asumsi yang terbentuk pada perumusan tujuan penelitian yang realistis dan bermanfaat. Tahapan ini dilakukan dengan melakukan studi literatur terkait faktor-faktor yang terlibat dalam penelitian. Hasil yang ditemukan kemudian dikembangkan menjadi deskripsi awal tentang situasi yang ada serta deskripsi tentang situasi yang diinginkan. Dalam tahap ini juga diterapkan kriteria yang dapat digunakan sebagai ukuran untuk mengevaluasi hasil penelitian (Blessing & Chakrabarti, 2009).

Penelitian diawali dengan memahami konsep dasar perlindungan data pribadi, regulasi yang berlaku saat ini, serta risiko yang dapat timbul dalam pengamanan informasi di lingkungan akademik dengan melibatkan studi literatur dan analisis dokumen terkait. Pada proses ini penelitian akan dimulai dengan kajian literatur yang mendalam mengenai Undang-Undang

Pelindungan Data Pribadi (UU PDP) serta keamanan informasi dalam institusi pendidikan tinggi.

3.2 Descriptive study I

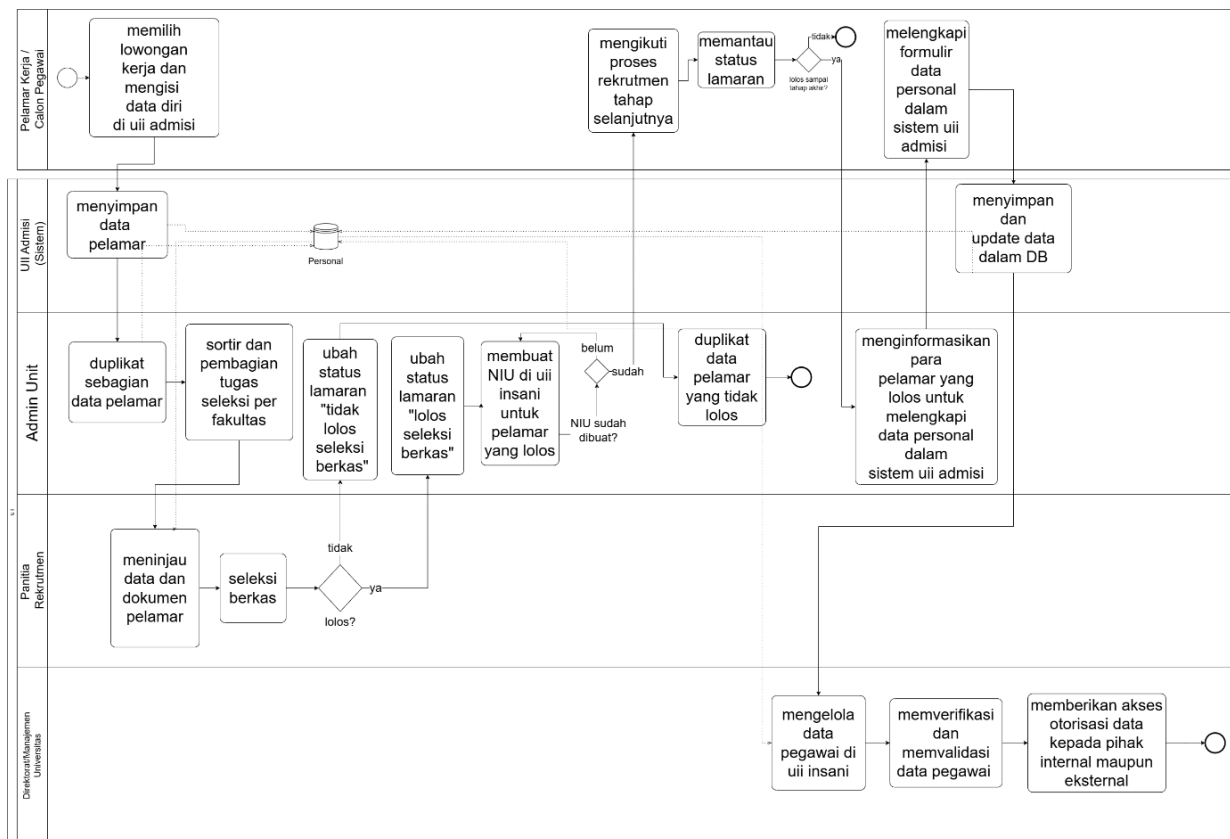
Studi literatur yang telah dilakukan sebelumnya memberikan pemahaman terkait desain dan faktor-faktor yang terlibat dalam penelitian. Hal ini berfungsi untuk mengidentifikasi faktor-faktor yang mempengaruhi objek penelitian untuk selanjutnya dianalisis agar mencapai titik paling efisien. Proses ini melibatkan penelitian empiris dengan melakukan pengamatan dan wawancara pada narasumber. Hasil berupa data hasil pengamatan dan transkrip wawancara kemudian dianalisis untuk mendapatkan pemahaman terkait karakteristik masalah yang belum terdefinisi dengan baik (Blessing & Chakrabarti, 2009).

Analisis Data Empiris adalah proses mempelajari dan menafsirkan informasi berdasarkan bukti yang digunakan. Proses ini bergantung pada data dan hasil nyata dari informasi yang didapatkan secara langsung. Analisis Data Empiris biasa digunakan untuk menemukan jawaban dengan pengamatan yang terukur. Analisis ini tidak pernah memberikan jawaban yang mutlak, melainkan menampilkan gambaran hal yang paling mungkin terjadi (Lee et al., 2021).

Dengan adanya Analisis Data Empiris dapat menjelaskan dan memahami berbagai karakteristik dari definisi berbagai masalah yang tidak memadai pada tahap research clarification, yang dapat di modifikasi agar mereka dapat memutuskan dari deskripsi yang ada dan cukup untuk melanjutkan ke tahap selanjutnya.

Fokus penelitian dimulai dengan menganalisis dan mengidentifikasi permasalahan utama yang terdapat di beberapa institusi pendidikan tinggi terkait pengamanan informasi, dan khususnya mengenai bagaimana Undang-Undang Pelindungan Data Pribadi (UU PDP) di implementasikan terhadap institusi pendidikan tinggi. Dengan observasi dan wawancara yang dilakukan terhadap Badan Sistem Informasi di UII menghasilkan bagaimana prosedur untuk pelamaran kerja dosen atau tenaga kependidikan yang ingin bekerja di Universitas Islam Indonesia yang diamankan oleh Badan Sistem Informasi UII terkait pengamanan informasi. Diawali dengan membuat janji terhadap Badan Sistem Informasi bagian ITSupport di hari pertama. Lalu di hari kedua dilanjutkan dengan membuat surat dan mengajukan kepada Kepala Badan Sistem Informasi melalui ITSupport Badan Sistem Informasi UII. Setelah surat diterima dan diperbolehkan pada hari ke tiga. Dilanjutkan dengan wawancara di hari ke empat terhadap narasumber yang menjadi kepala yang memegang tanggung jawab di bidang UIIINSANI. UIIINSANI sendiri adalah fitur yang ada di dalam UIIGateway yang menyimpan data pribadi

para dosen dan tenaga kependidikan. Lalu didapatkan bagaimana gambaran mengenai prosedur yang saat ini digunakan melalui hasil rekaman wawancara. Hasil dari tahap ini adalah gambaran bagaimana prosedur terkait pelamaran kerja dosen atau tenaga pendidikan yang ingin bekerja di Universitas Islam Indonesia. Lalu, menghasilkan diagram berupa BPMN yang menggambarkan prosedur keamanan informasi yang sedang diterapkan dan ditampilkan di gambar 3.2 Diagram BPMN dari Sistem UIIADMISI saat ini.



Gambar 3. 2 Diagram BPMN dari Sistem UIIADMISI saat ini

3.3 Prescriptive Study

Pada tahap Prescriptive Study, dengan memahami lebih dalam tentang situasi yang ada agar dapat memperbaiki dan memperjelas deskripsi sesuai situasi yang diinginkan. Oleh karena itu, dapat digambarkan visi ketika terdapat beberapa faktor dalam situasi yang ada dengan situasi yang diinginkan sehingga dapat memutuskan situasi apa yang lebih baik diwujudkan. Lalu dapat mengembangkan berbagai kemungkinan skenario dengan memvariasikan faktor faktor yang dituju, sehingga dapat memutuskan dan meningkatkan kualitas definisi masalah sebagai faktor utama untuk diperbaiki. (Blessing & Chakrabarti, 2009)

Dengan pemahaman yang cukup matang, dapat dimulai melalui pengembangan sistematis untuk meningkatkan kualitas definisi masalah. Dengan menggunakan berbagai faktor yang saling terkait dimulai dari Descriptive Study 1, deskripsi situasi yang diinginkan telah berkembang dengan baik, sehingga dapat mengikuti metodologi desain dengan sistematis dibantu oleh beberapa faktor pada tahap sebelumnya.

Berdasarkan hasil analisis dari tahap sebelumnya, fokus pada tahap penelitian ini adalah mengusulkan perbaikan terhadap model keamanan informasi yang lebih selaras dengan ketentuan UU PDP. Proses ini menghasilkan bagaimana gambaran baru BPMN yang telah dibuat dan disesuaikan dengan ketentuan UU PDP agar proses lebih aman dan efektif dalam melindungi data pribadi di UII. Proses ini mempertimbangkan beberapa aspek yaitu kepatuhan terhadap regulasi, pencegahan risiko, serta efisiensi operasional dalam institusi pendidikan tinggi.

3.4 Descriptive Study II

Dengan melanjutkan penyelidikan dari deskripsi situasi yang diinginkan dengan disusun secara sistematis untuk mewujudkan situasi yang diinginkan dilakukan dua studi empiris untuk memahami situasi yang ingin diwujudkan tersebut.

1. Studi Pertama akan digunakan untuk mengevaluasi sejauh mana situasi tersebut jika diterapkan. Pertanyaan utama dalam studi ini adalah bagaimana jika situasi tersebut dapat digunakan jika definisi masalah yang berkualitas tinggi.
2. Studi Kedua akan digunakan untuk mengevaluasi kemungkinan keberhasilan situasi jika diwujudkan. Berdasarkan faktor yang dikembangkan sebelumnya. Pertanyaan utama dalam studi ini adalah apakah waktu yang digunakan untuk modifikasi situasi tersebut efektif.

Hasil dari kedua studi akan menampilkan bahwa situasi tersebut dapat diwujudkan, namun jika situasi tidak memenuhi harapan, hal ini bisa disebabkan ketika situasi tersebut melampaui batas yang telah dikembangkan. Kejadian seperti ini kerap terjadi seperti beberapa efek yang tidak diantisipasi sebelumnya. Konsep yang telah dikembangkan tidak dapat langsung disimpulkan bahwa konsep tersebut cukup menjanjikan, tetapi harus adanya hal yang ditingkatkan melalui penelitian lebih lanjut tentang situasi yang harus diantisipasi agar dapat disesuaikan kembali sebelum situasi ini dapat diperbaiki lebih lanjut (Blessing & Chakrabarti, 2009)

Pada tahap ini, model BPMN yang telah dibuat dan diusulkan akan dievaluasi oleh pemangku kepentingan yang relevan berdasarkan umpan balik, termasuk Badan Sistem

Informasi UII. Evaluasi ini bertujuan untuk menilai bagaimana model yang diusulkan dapat diterapkan di lingkungan institusi, serta dampaknya terhadap manajemen risiko keamanan informasi. Hasil dari evaluasi ini akan menjadi dasar untuk menyusun kesimpulan dan saran lebih lanjut bagi institusi pendidikan tinggi dalam penerapan strategi mengenai keamanan informasi terkait perlindungan data pribadi yang sesuai dengan ketentuan hukum yang berlaku.

BAB IV

ANALISIS DAN PEMBAHASAN

4.1 Analisis Regulasi dan Risiko Dalam Pengamanan Informasi

Pada tahap ini menjelaskan bahwa regulasi yang ditulis di dalam Undang-Undang Pelindungan Data Pribadi (UU PDP) menekankan terhadap pentingnya pelindungan data pribadi, termasuk hak subjek data, kewajiban pengendali data, dan sanksi bagi pelanggaran, serta risiko yang mungkin terjadi dalam pengamanan informasi di institusi pendidikan tinggi. Karena data yang dikelola oleh institusi pendidikan tinggi meliputi data para mahasiswa, dosen, dan tenaga pendidikan. Hal itu sangat rentan terhadap risiko kebocoran data dan serangan siber.

Dengan memahami regulasi dan risiko berdasarkan yang tertulis di Undang-Undang Pelindungan Data Pribadi (UU PDP), institusi pendidikan tinggi dapat merancang strategi dalam pengamanan informasi data pribadi di lingkungan akademik yang lebih efektif. Beberapa langkah-langkah seperti penerapan enkripsi data untuk autentikasi admin, pop-up terhadap setiap pengguna jika data sedang diolah, serta permintaan persetujuan kepada para pengguna jika data para pengguna akan disimpan oleh kampus untuk membantu mengurangi risiko kebocoran data dan serangan siber, serta memastikan kepatuhan terhadap Undang-Undang Pelindungan Data Pribadi (UU PDP).

4.2 Kondisi Sistem Saat Ini Pada Keamanan Informasi Di UII

Berdasarkan observasi dan wawancara dengan Badan Sistem Informasi UII. Telah dibuat dokumentasi berupa *Business Process Model and Notation* (BPMN) terkait prosedur pengamanan informasi yang dilakukan Badan Sistem Informasi UII saat ini. Beberapa pasal Undang-Undang Pelindungan Data Pribadi sudah diimplementasikan pada sistem UIIADMISI seperti pada Pasal 16 Undang-Undang Pelindungan Data Pribadi yang berbunyi “Pemrosesan Data Pribadi meliputi: pemerolehan dan pengumpulan, pengolahan dan penganalisisan, penyimpanan, perbaikan dan pembaruan, penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan, dan/atau penghapusan atau pemusnahan” yang menjelaskan cakupan dari Pemrosesan Data Pribadi di dalam sistem UIIADMISI saat ini. Oleh karena itu, masih terdapat beberapa kekurangan yang perlu diperbaiki agar sesuai dengan Undang-Undang Pelindungan Data Pribadi (UU PDP), seperti tidak adanya hak subjek data pribadi, tidak adanya transparansi antara pengendali data pribadi dan subjek data pribadi sesuai dengan pasal 30 ayat 1 Undang-

Undang Data Pribadi (UU PDP) yang berbunyi “Pengendali Data Pribadi wajib memperbarui dan/ atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi paling lambat 3 x 24 (tiga kali dua puluh empat) jam terhitung sejak Pengendali Data Pribadi menerima permintaan pembaruan dan/atau perbaikan Data Pribadi.”, dan persetujuan eksplisit kepada Subjek Data Pribadi terkait perizinan pengolahan data oleh pengendali data pribadi sesuai dengan pasal 20 ayat 2 Undang-Undang Pelindungan Data Pribadi (UU PDP) yang berbunyi “persetujuan yang sah secara eksplisit dari Subjek Data Pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan oleh Pengendali Data Pribadi kepada Subjek Data Pribadi”. Oleh karena itu, diwajibkan adanya persetujuan yang sah secara eksplisit dari subjek data pribadi sebelum pemrosesan data dilakukan.

Model BPMN terkait pengamanan informasi yang dilakukan oleh Badan Sistem Informasi saat ini dibuat dengan menggunakan salah satu website yaitu *draw.io*. dapat dilihat pada gambar 4.1 diagram BPMN ditampilkan dengan lima *swimlane* yang masing-masing terdiri dari pelamar kerja, UIIAdmisi (sistem), Admin unit, panitia rekrutmen, dan Direktorat/manajemen Universitas. Pelamar kerja diartikan sebagai orang yang ingin mendaftarkan dirinya sebagai tenaga pendidikan atau dosen di UII. Selanjutnya terdapat Admin unit yang berperan sebagai orang yang dapat menduplikat data para pelamar dan menginformasikan para pelamar kerja yang lolos atau tidak lolos di UII selama sesi pendaftaran. Dan terdapat Panitia Rekrutmen yang berperan sebagai orang yang meninjau data dan dokumen para pelamar serta menyeleksi berkas para pelamar. Sedangkan Direktorat/manajemen Universitas berperan sebagai pihak berwenang yang dapat mengelola data para pegawai, memverifikasi dan memvalidasi data para pegawai, serta memberikan akses otorisasi data kepada pihak internal maupun eksternal. UIIAdmisi (Sistem) digunakan sebagai penghubung antara para pelamar kerja dengan Admin Unit dalam mengirim atau menerima data. Sedangkan Personal adalah sebuah database untuk menyimpan data dan dokumen para pegawai.

Berikut ini adalah beberapa gambar yang menunjukkan bagaimana berkas pegawai yang lebih komprehensif seperti, berkas administratif, ijazah, SK, dan dokumen lainnya dikelola dalam sistem yang digunakan saat ini di UII dan digunakan oleh manajemen dalam proses verifikasi dan administrasi:

UNIVERSITAS ISLAM INDONESIA

Insani > Personal

Udah personal

Proses pengisian data 20%

Alamat identitas (KTP)

Provinsi: Kota/Kabupaten:
 Kecamatan: Desa/Kelurahan:
 RT: RW: Dusun:
 Alamat lengkap:
 Kode POS: Nomor telepon rumah:
 Status tinggal:

Alamat domisili

☐ Sama dengan alamat KTP

Provinsi: Kota/Kabupaten:
 Kecamatan: Desa/Kelurahan:
 RT: RW: Dusun:
 Alamat lengkap:
 Kode POS: Nomor telepon rumah:
 Status tinggal:

Alamat orang tua

☐ Sama dengan alamat KTP

Provinsi: Kota/Kabupaten:
 Kecamatan: Desa/Kelurahan:
 RT: RW: Dusun:
 Alamat lengkap:
 Kode POS: Nomor telepon rumah:
 Status tinggal:

Alamat Kantor (jika ada)

Provinsi: Kota/Kabupaten:
 Kecamatan: Desa/Kelurahan:
 RT: RW: Dusun:
 Alamat lengkap:
 Kode POS: Nomor telepon rumah:
 Status tinggal:

Batal Simpan

Gambar 4. 2 Halaman Edit Data Diri Pegawai (1)

UNIVERSITAS ISLAM INDONESIA

> Insani > Personal

Uji Kinerja

Personal

Kepegawaian

Surat tugas

Surat Keputusan

Evaluasi

Penghargaan

Simpeg

Ubah personal

Menunggu

Data identitas diri anda sedang dalam proses pemeriksaan

Kewarganegaraan *

WNA

Paspor

File foto paspor

Unggah

Maks 2 MB
Format jpg/png/ang

Nomor paspor

KTP

File foto KTP

Unggah

Maks 2 MB
Format jpg/png/ang

Nomor induk Kependudukan (NIK)

BPJS kesehatan

File BPJS kesehatan

Unggah

Maks 2 MB
Format jpg/png/ang

Nomor BPJS kesehatan

BPJS ketenagakerjaan

File BPJS ketenagakerjaan

Unggah

Maks 2 MB
Format jpg/png/ang

Nomor BPJS ketenagakerjaan

NPWP

File NPWP

Unggah

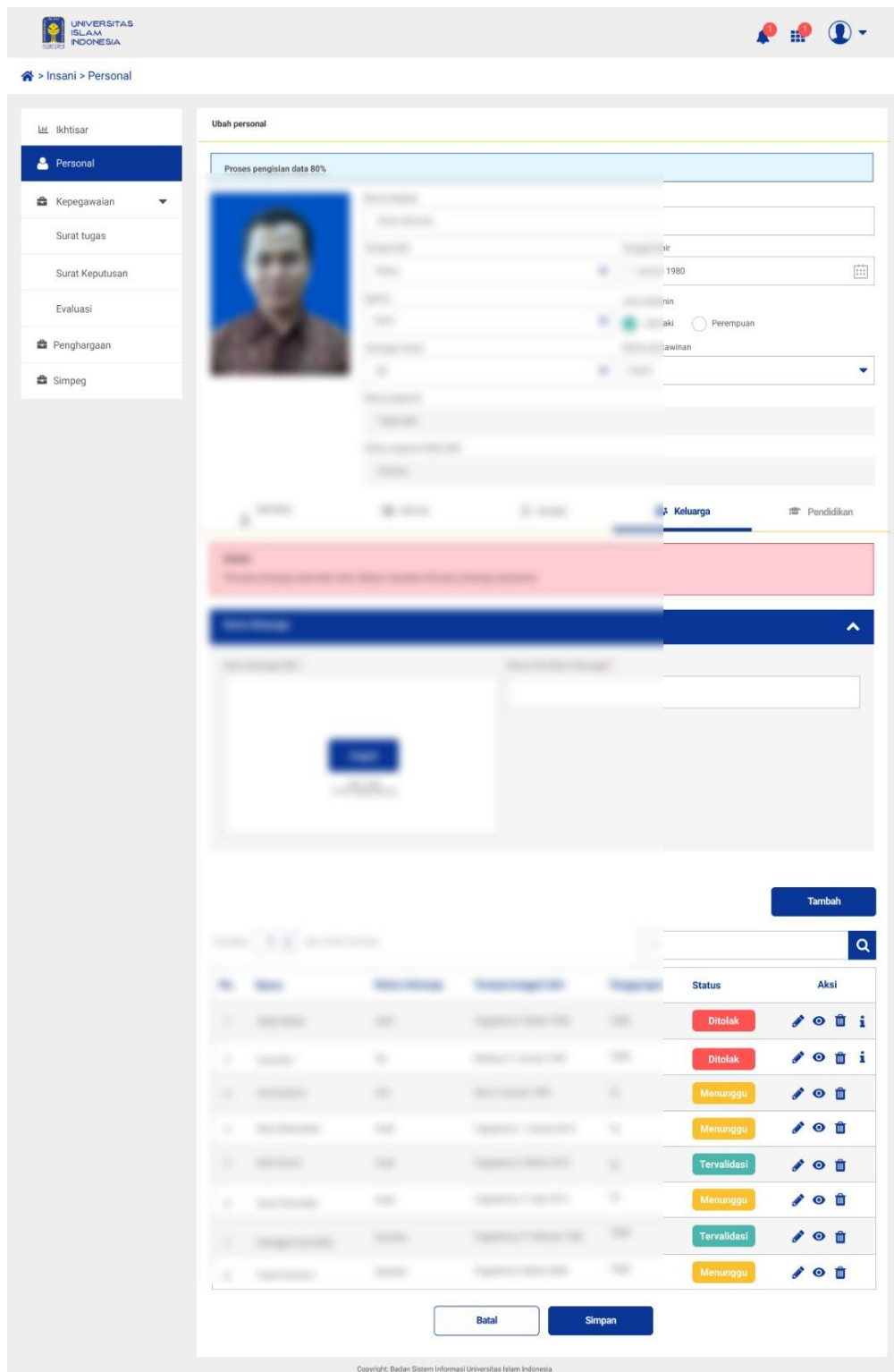
Maks 2 MB
Format jpg/png/ang

Nomor NPWP

Batal

Simpan

Gambar 4. 3 Halaman Edit Data Diri Pegawai (2)



Gambar 4. 4 Halaman Update Data Diri Pegawai (3)

Tambah pendidikan

Lokasi institusi
☐ Dalam negeri ☒ Luar negeri

Jenis studi: SS Nama institusi: University of Adelaide

Jurusan: Informatics Engineering Konsentrasi/Field of Study: Data science Akreditasi: A

Tahun masuk: Gelar: M.Eng Nomor induk: 13023001

Jumlah tugas akhir / Thesis / Disertasi: Data science analytics

Berkas pendukung

Jenis berkas pendukung: Surat

Nomor surat: 00100117 Tanggal kelulusan: 30 Januari 2018

Tanggal surat: 30 Februari 2018 Nilai IPK: 5.00 Jumlah pengajaran/SKS: 144

Format file pdf maksimal 2MB

Unggah ☒ surat.pdf 194.6 KB

Jenis berkas pendukung: Penyetaraan

Nomor SK penyetaraan: 00100117 Tanggal SK penyetaraan: 30 Januari 2018

Format file pdf maksimal 2MB

Unggah ☒ sk-penyetaraan.pdf 194.6 KB

Jenis berkas pendukung:

Batal Simpan

Gambar 4. 5 Halaman Update Data Pendidikan Pegawai (4)

Selain itu, gambar-gambar berikut juga menggambarkan tampilan sistem yang digunakan saat ini seperti informasi data pribadi di UII dan pemahaman lebih dalam mengenai pengelolaan informasi pegawai.

Detail pendidikan

Lokasi institusi	Darmasri
Jenjang studi	S1
Nama institusi	Universitas Islam Indonesia
Jurusan	Teknik Informatika
Konsentrasi/kebidanan	Data science
Alamat	A
Tahun masuk	2013
Gelar	S.Kom
Nomor induk	12020001
Judul tugas akhir/tesis/disertasi	Analisis data rekam medis di RS. Sanglah
Berkas pendidikan	
Jenis berkas pendidikan	Skripsi
Nomor skripsi	0000017
Tanggal kelulusan	20 Januari 2018
Tanggal skripsi	20 Februari 2018
Nilai IPK	5,00
Jumlah pelajaran/SKI	144
Berkas skripsi	skripsi.pdf 746.6 KB
Jenis berkas pendidikan	Penyerahan
Nomor SK penyerahan	0000017
Tanggal SK Penyerahan	20 Januari 2018
Berkas skripsi	skripsi.pdf 746.6 KB

[Kembali](#)

No	Status	Nama Institusi	Jurusan	Tahun Masuk	Tahun Keluar	Aksi
1.	Status 1	Universitas Islam Indonesia Yogyakarta	Teknik Informatika	2013	2018	Edit Hapus
2.	Status 1	Universitas Islam Indonesia Yogyakarta	Teknik Informatika	2013	2018	Edit Hapus

Copyright Sistem Sistem Informasi Universitas Islam Indonesia

Gambar 4. 6 Informasi data pribadi di UIIADMISI

Detail keluarga

NIK (Nomor Induk Kependudukan)	3206021713410002
Nama	Muhammad
Tempat, tanggal lahir	Yogyakarta, 21 Juli 1991
Agama	Islam
Jenis kelamin	Pemahaman
Status perkawinan	Kawin
Golongan darah	A+
Hubungan anggota keluarga	Suami
Pendidikan terakhir	S1
Pekerjaan	Widyawisata
Tanggungan keluarga	Tidak
Tanggungan PTSP	Tidak
Tanggungan kesehatan	Tidak
Meninggal	Tidak
Berkas pendidikan	
Akta kelahiran	akta_kelahiran.pdf 746.6 KB
Akta nikah	akta_nikah.pdf 746.6 KB
Kartu keluarga	kartu_keluarga.pdf 746.6 KB

[Kembali](#)

Widyawisata
Pemerintah dan swasta

[Kembali](#) [Simpan](#)

Status perkawinan

Gambar 4. 7 Informasi Data Pribadi di UIIADMISI

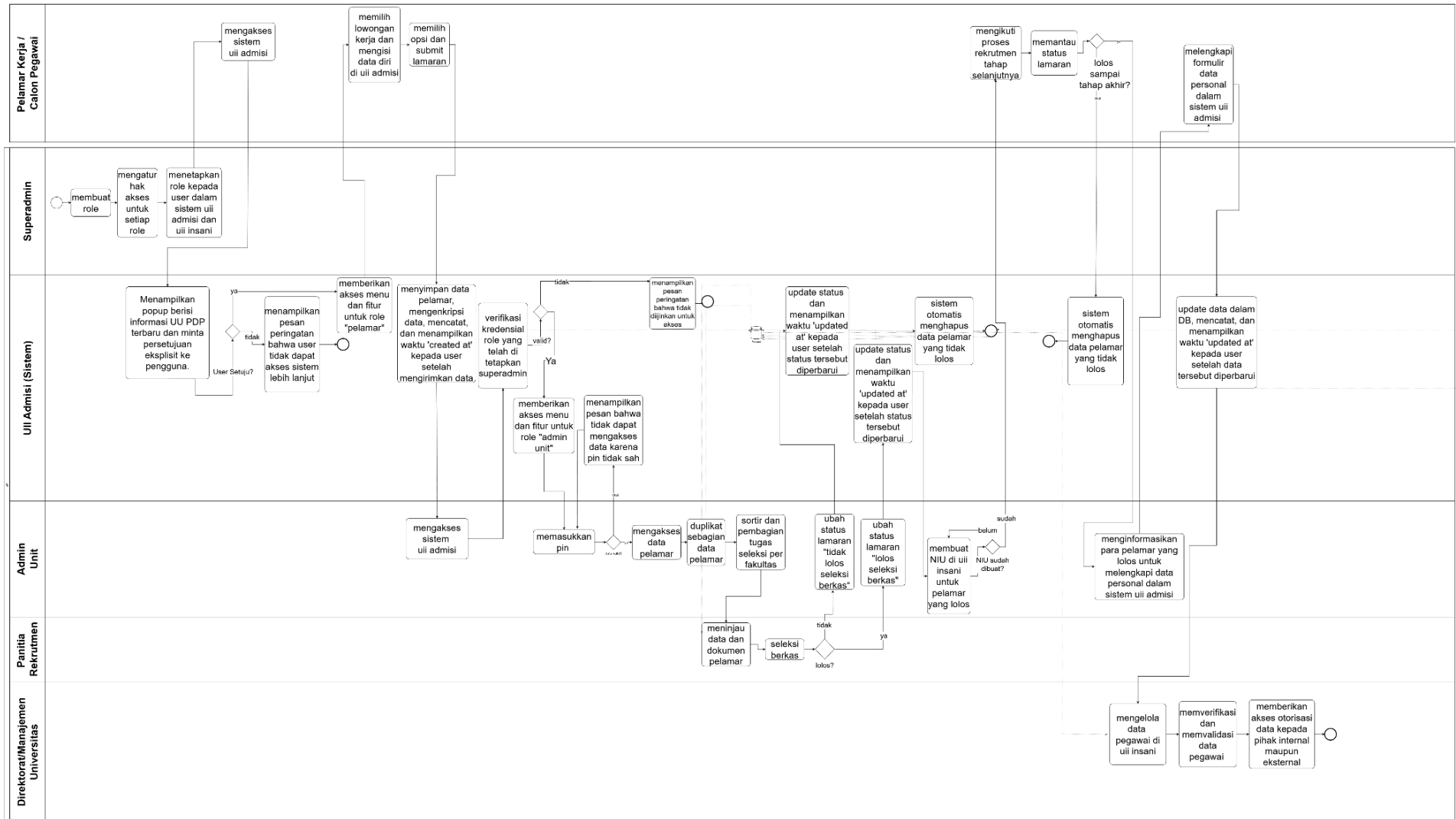
Gambar 4.6 dan 4.7 memberikan gambaran yang cukup jelas tentang bagaimana informasi pegawai dikelola oleh sistem yang digunakan saat ini oleh UII sekaligus menjadi bahan untuk analisis dan perbaikan sistem dalam rangka memenuhi standar yang ditetapkan oleh Undang-Undang No 27 Tahun 2022 tentang Pelindungan Data Pribadi.

4.3 Perancangan Model BPMN yang Diusulkan

Kemudian setelah menemukan dan mengidentifikasi dari permasalahan yang ada di BPMN saat ini dipakai, telah dirancang model BPMN yang diusulkan kepada Badan Sistem Informasi untuk diimplementasikan ke UII yang sudah mencakup berdasarkan ketentuan UU PDP. Dengan dibuatnya BPMN ini, diharapkan UII dapat meningkatkan kepatuhan terhadap regulasi yang tertulis di dalam UU PDP dan mengurangi risiko keamanan informasi seperti kebocoran data.

BPMN yang diusulkan dapat dilihat pada gambar 4.8 yang menggambarkan keseluruhan proses bisnis sesuai dengan uraian berikut:

PROPOSE



Gambar 4. 8 Diagram BPMN yang di propose untuk UIIADMISI

Proses bisnis terkait pengamanan informasi yang saya usulkan untuk UII bisa dilihat pada Gambar 4.8 yang menampilkan enam swimlane yang masing-masing terdiri dari Pelamar kerja, Superadmin, UIIAdmisi (Sistem), Admin Unit, Panitia Rekrutmen, serta Direktorat dan Manajemen Universitas. Pelamar kerja diartikan sebagai orang yang ingin mendaftarkan dirinya sebagai tenaga pendidikan atau dosen di UII. Selanjutnya terdapat Superadmin yang diartikan sebagai Pihak berwenang yang berhak menentukan setiap role untuk mengelola hak akses data pribadi di dalam sistem. Lalu terdapat UIIADMISI yang diartikan sebagai sistem yang digunakan oleh calon pegawai untuk mendaftar sebagai dosen atau tenaga pendidikan. Sedangkan Admin unit yang berperan sebagai orang yang dapat mengakses data di sistem UIIAdmisi dan menduplikat data para pelamar, serta menginformasikan para pelamar kerja yang lolos atau tidak lolos di UII selama sesi pendaftaran. Dan terdapat Panitia Rekrutmen yang berperan sebagai orang yang meninjau data dan dokumen para pelamar serta menyeleksi berkas para pelamar. Sedangkan Direktorat/manajemen Universitas berperan sebagai pihak berwenang yang dapat mengelola data para pegawai, memverifikasi dan memvalidasi data para pegawai, serta memberikan akses otorisasi data kepada pihak internal maupun eksternal. UIIAdmisi (Sistem) digunakan sebagai penghubung antara para pelamar kerja dengan Admin Unit dalam mengirim atau menerima data. Sedangkan Personal adalah sebuah database untuk menyimpan data dan dokumen para pegawai.

Mulanya Superadmin membuat role untuk mengatur hak akses kepada setiap role agar ditetapkan role kepada setiap user dalam sistem UIIAdmisi. Selanjutnya para pelamar kerja mengakses sitem UIIAdmisi. Lalu sistem UIIAdmisi akan menampilkan kebijakan baru UU PDP dan meminta persetujuan secara eksplisit kepada user, jika user tidak setuju sistem akan menampilkan pesan peringatan bahwa user tidak dapat akses sistem lebih lanjut. Tetapi, jika user setuju sistem akan memberikan akses menu dan fitur untuk role sebagai “pelamar”. Selanjutnya para pelamar kerja memilih lowongan kerja dan mengisi data diri di UIIAdmisi. Setelah data diisi oleh para pelamar, sistem akan menampilkan pop up yang memberikan opsi kepada pemilik data untuk meminta akses untuk mengajukan penghapusan data pemilik. Setelah para pelamar memilih opsi dan submit lamaran, sistem akan menyimpan data pelamar, mengenkripsi data, mencatat, dan menampilkan waktu ‘created at’ kepada user setelah mengirimkan data. Selanjutnya Admin Unit akan mengakses dan sistem akan memverifikasi kredensial role yang telah ditetapkan oleh superadmin. Jika verifikasi tidak valid sistem akan menampilkan pesan peringatan bahwa tidak diizinkan untuk akses. Lalu jika verifikasi valid, sistem akan memberikan akses menu dan fitur untuk role “Admin Unit”. Selanjutnya Admin

Unit akan memasukkan pin, jika pin yang dimasukkan tidak valid maka sistem akan menampilkan pesan peringatan bahwa “tidak dapat mengakses data karena pin tidak sah”. Sebaliknya jika pin yang dimasukkan valid maka Admin Unit dapat mengakses data para pelamar dan menduplikat sebagian data pelamar serta menyortir dan membagi tugas seleksi per fakultas. Kemudian Panitia rekrutmen meninjau data dan dokumen para pelamar dan menyeleksi berkas, jika tidak lolos Admin Unit akan mengubah status lamaran menjadi “tidak lolos seleksi berkas” dan sistem mengupdate, mencatat, dan menampilkan kepada user setelah status tersebut diperbarui, serta otomatis menghapus data para pelamar yang tidak lolos. Sedangkan jika lolos Admin Unit akan mengubah status lamaran menjadi “lolos seleksi berkas”, lalu sistem akan mengupdate, mencatat, dan menampilkan kepada user setelah status tersebut diperbarui. Selanjutnya Admin Unit akan membuat NIU di UIIInsani untuk pelamar yang lolos. Kemudian para pelamar melanjutkan untuk mengikuti proses rekrutmen tahap selanjutnya dan memantau status lamaran. Jika para pelamar tidak lolos sampai tahap akhir, sistem akan mengupdate, mencatat, dan menampilkan kepada user setelah status tersebut diperbarui, serta sistem otomatis menghapus data para pelamar yang tidak lolos. Sedangkan jika lolos Admin Unit akan menginformasikan para pelamar yang lolos untuk melengkapi data personal dalam sistem UIIAdmisi. Kemudian setelah para pelamar melengkapi formulir data personal dalam sistem UIIAdmisi, sistem akan mengupdate data dalam database, mencatat, dan menampilkan ‘updated at’ kepada user setelah data tersebut diperbarui. Selanjutnya pihak berwenang yang relevan seperti Direktorat dan Manajemen Universitas mempunyai hak untuk mengelola data pegawai di UIIInsani, memverifikasi dan memvalidasi data pegawai, serta memberikan akses otorisasi data kepada pihak internal maupun eksternal.

4.4 Implementasi Sistem Antarmuka Berdasarkan Model BPMN

Sebelum dijelaskan bagaimana alur proses bisnis melalui model BPMN, berikut ini adalah tampilan mengenai fitur-fitur yang diusulkan untuk sistem UII saat ini serta mendukung perlindungan data pribadi di lingkungan institusi pendidikan tinggi.

4.4.1 Persetujuan Eksplisit Ke Pengguna Terhadap Kebijakan Undang-Undang Pelindungan Data Pribadi

Pada Gambar 4.9 sampai Gambar 4.13 memperlihatkan mekanisme konfirmasi persetujuan eksplisit dari pengguna terhadap kebijakan pelindungan data pribadi. Hal ini sejalan dengan pasal 20 ayat 2 Undang-Undang Pelindungan Data Pribadi yang berbunyi “persetujuan yang sah secara eksplisit dari Subjek Data Pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan oleh Pengendali Data Pribadi kepada Subjek Data Pribadi”. Oleh karena itu, Undang-Undang Pelindungan Data Pribadi mewajibkan adanya persetujuan yang sah secara eksplisit dari Subjek Data Pribadi sebelum pemrosesan data dilakukan.



Gambar 4. 9 Persetujuan eksplisit ke pengguna (1)



B. Jenis Data Pribadi

UU PDP membagi data pribadi menjadi dua jenis. Kami memproses kedua jenis data tersebut untuk menunjang operasional pendidikan, penelitian, dan administrasi.

- **Data Pribadi Bersifat Umum:** Meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, serta data pribadi lain yang dikombinasikan untuk mengidentifikasi seseorang seperti, Nomor Induk Dosen Nasional (NIDN), Nomor Induk Kependudukan (NIK), alamat rumah, nomor telepon, dan alamat email Anda.
- **Data Pribadi Bersifat Spesifik:** Meliputi data dan informasi kesehatan, catatan kejahatan, data anak, data keuangan pribadi, dan/atau data lainnya sesuai ketentuan perundang-undangan. Pemrosesan data jenis ini dilakukan dengan tingkat kehati-hatian dan keamanan yang lebih tinggi karena potensi risikonya yang lebih besar.

C. Pemrosesan Data Pribadi

Pemrosesan data pribadi di institusi kami mencakup seluruh siklus hidup data Anda, yang dilakukan untuk tujuan yang sah dan relevan dengan penyelenggaraan pendidikan tinggi. Proses ini meliputi:

- **Pemerolehan dan Pengumpulan:** Kami mengumpulkan data langsung dari Anda saat pengisian formulir pendaftaran online melalui sistem informasi akademik.
- **Pengolahan dan Analisis:** Data kehadiran dianalisis untuk pemenuhan syarat ujian, dan data lainnya dianalisis untuk peningkatan kualitas layanan pendidikan.
- **Penyimpanan:** Data Anda disimpan dalam basis data yang aman, baik di server fisik maupun cloud, dengan

Gambar 4. 10 Persetujuan eksplisit ke pengguna (2)



menyimpan data Anda dalam sistem yang aman.

- **Perbaikan dan Pembaruan:** Kami memfasilitasi pembaruan data Anda untuk memastikan akurasi, misalnya perubahan alamat atau nomor kontak.
- **Penampilan, Pengumuman, atau Pengungkapan:** Kami dapat menampilkan nama dan status kelulusan Anda dalam daftar yudisium. Pengungkapan data kepada pihak lain hanya dilakukan berdasarkan dasar hukum yang sah.
- **Penghapusan atau Pemusnahan:** Data akan dihapus atau dimusnahkan ketika masa retensinya berakhir atau atas permintaan Anda sesuai dengan hak yang diatur dalam UU PDP.

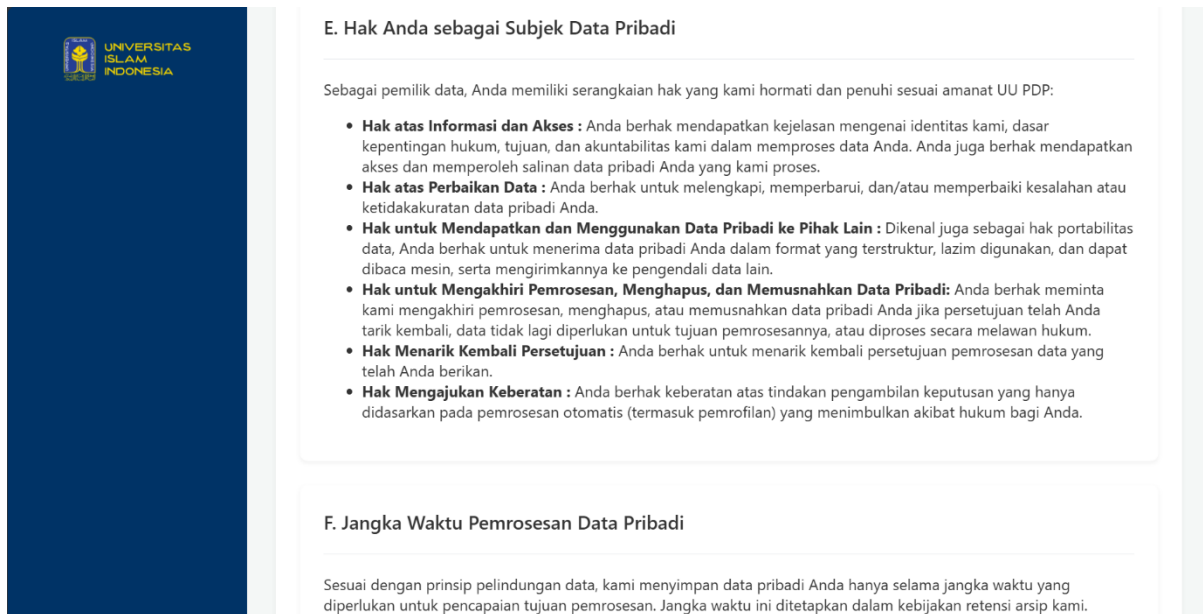
D. Pengendalian dan Transfer Data Pribadi

Universitas bertindak sebagai **Pengendali Data Pribadi**. Dalam peran ini, kami yang menentukan tujuan dan melakukan kontrol atas pemrosesan data pribadi Anda. Kami bertanggung jawab penuh untuk memastikan seluruh pemrosesan data sesuai dengan prinsip-prinsip perlindungan data pribadi.

Transfer data pribadi dapat terjadi dalam dua lingkup:

- **Internal:** Data ditransfer antar unit di dalam universitas melalui sistem informasi yang terintegrasi dan aman untuk menunjang proses bisnis internal.
- **Eksternal:** Kami dapat mentransfer data Anda ke pihak ketiga, seperti ke Pangkalan Data Pendidikan Tinggi (PDDikti) sebagai kewajiban pelaporan kepada pemerintah, atau ke lembaga akreditasi. Transfer ini hanya dilakukan jika: (1) ada dasar hukum yang jelas, (2) didasari persetujuan Anda jika diperlukan, dan (3) kami telah memastikan pihak penerima memiliki standar perlindungan data yang setara atau lebih tinggi dari yang kami terapkan.

Gambar 4. 11 Persetujuan eksplisit ke pengguna (3)



E. Hak Anda sebagai Subjek Data Pribadi

Sebagai pemilik data, Anda memiliki serangkaian hak yang kami hormati dan penuhi sesuai amanat UU PDP:

- **Hak atas Informasi dan Akses** : Anda berhak mendapatkan kejelasan mengenai identitas kami, dasar kepentingan hukum, tujuan, dan akuntabilitas kami dalam memproses data Anda. Anda juga berhak mendapatkan akses dan memperoleh salinan data pribadi Anda yang kami proses.
- **Hak atas Perbaikan Data** : Anda berhak untuk melengkapi, memperbarui, dan/atau memperbaiki kesalahan atau ketidakakuratan data pribadi Anda.
- **Hak untuk Mendapatkan dan Menggunakan Data Pribadi ke Pihak Lain** : Dikenal juga sebagai hak portabilitas data, Anda berhak untuk menerima data pribadi Anda dalam format yang terstruktur, lazim digunakan, dan dapat dibaca mesin, serta mengirimkannya ke pengendali data lain.
- **Hak untuk Mengakhiri Pemrosesan, Menghapus, dan Memusnahkan Data Pribadi**: Anda berhak meminta kami mengakhiri pemrosesan, menghapus, atau memusnahkan data pribadi Anda jika persetujuan telah Anda tarik kembali, data tidak lagi diperlukan untuk tujuan pemrosesannya, atau diproses secara melawan hukum.
- **Hak Menarik Kembali Persetujuan** : Anda berhak untuk menarik kembali persetujuan pemrosesan data yang telah Anda berikan.
- **Hak Mengajukan Keberatan** : Anda berhak keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan otomatis (termasuk pemprofilan) yang menimbulkan akibat hukum bagi Anda.

F. Jangka Waktu Pemrosesan Data Pribadi

Sesuai dengan prinsip perlindungan data, kami menyimpan data pribadi Anda hanya selama jangka waktu yang diperlukan untuk pencapaian tujuan pemrosesan. Jangka waktu ini ditetapkan dalam kebijakan retensi arsip kami.

Gambar 4. 12 Persetujuan eksplisit ke pengguna (4)



F. Jangka Waktu Pemrosesan Data Pribadi

Sesuai dengan prinsip perlindungan data, kami menyimpan data pribadi Anda hanya selama jangka waktu yang diperlukan untuk pencapaian tujuan pemrosesan. Jangka waktu ini ditetapkan dalam kebijakan retensi arsip kami. Secara umum, data akademik inti akan disimpan dalam jangka waktu yang sangat panjang sesuai dengan kebutuhan penyelenggaraan pendidikan dan peraturan perundang-undangan. Namun, untuk data lain yang bersifat penunjang, akan kami hapus atau musnahkan setelah tidak lagi relevan atau setelah masa retensi berakhir. Contohnya, data log akses internet Anda akan dihapus secara berkala. Setelah masa studi Anda berakhir, sebagian data akan tetap kami simpan untuk keperluan alumni dan pelaporan, namun sebagian lainnya yang tidak lagi relevan akan dimusnahkan secara aman.

Persetujuan Anda

☐ Saya dengan ini menyatakan telah membaca, memahami, dan menyetujui seluruh ketentuan dalam Kebijakan UU PDP.

[Lanjutkan](#) [Kembali](#)

Gambar 4. 13 Persetujuan Eksplisit ke pengguna (5)

Pada halaman ini memperlihatkan mekanisme konfirmasi persetujuan eksplisit dari pengguna terhadap kebijakan perlindungan data pribadi. Hal ini sejalan dengan pasal 20 ayat 2 UU PDP yang mewajibkan adanya persetujuan yang sah secara eksplisit dari Subjek Data Pribadi sebelum pemrosesan data dilakukan.

4.4.2 Autentikasi Admin

Gambar 4.14 menampilkan tampilan autentikasi tambahan berupa PIN 6 digit yang harus dimasukkan oleh admin sebelum dapat mengakses *dashboard* sistem. Fitur ini merupakan bagian dari mekanisme perlindungan data pribadi dan pengendalian akses di lingkungan

institusi pendidikan tinggi. Secara prinsip, autentikasi PIN ini mendukung implementasi asas kerahasiaan, integritas, dan akses yang terbatas yang diatur dalam Pasal 39 ayat 1 UU No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi yang berbunyi “Pengendali Data Pribadi wajib mencegah Data Pribadi diakses secara tidak sah”.

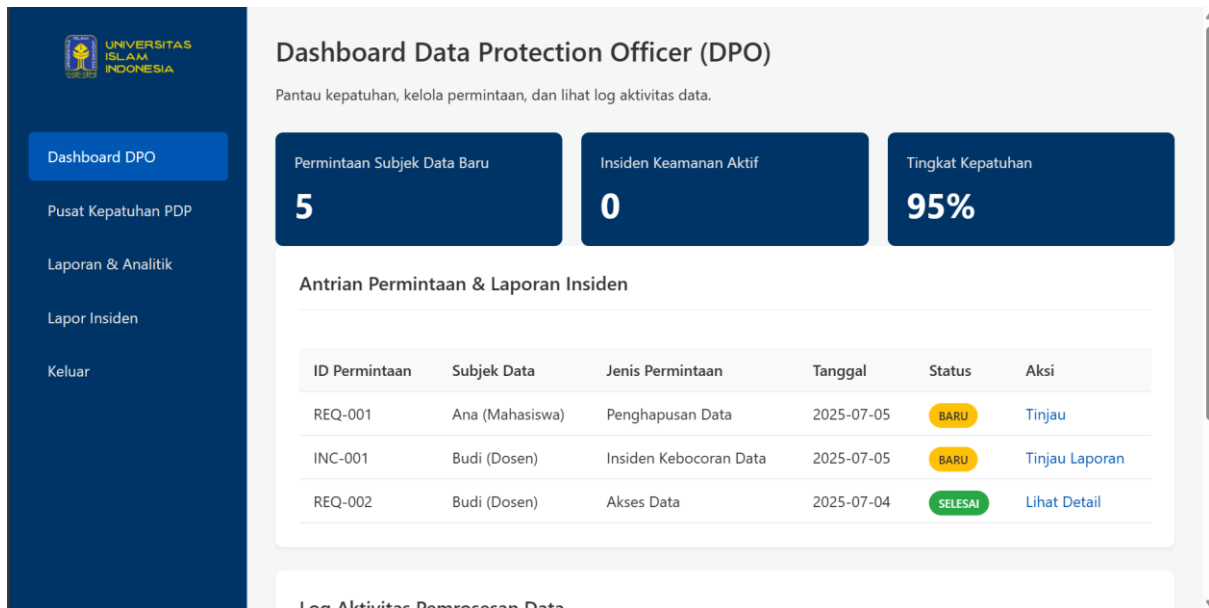
Gambar 4. 14 Autentikasi Admin Unit

4.4.3 Fitur DPO

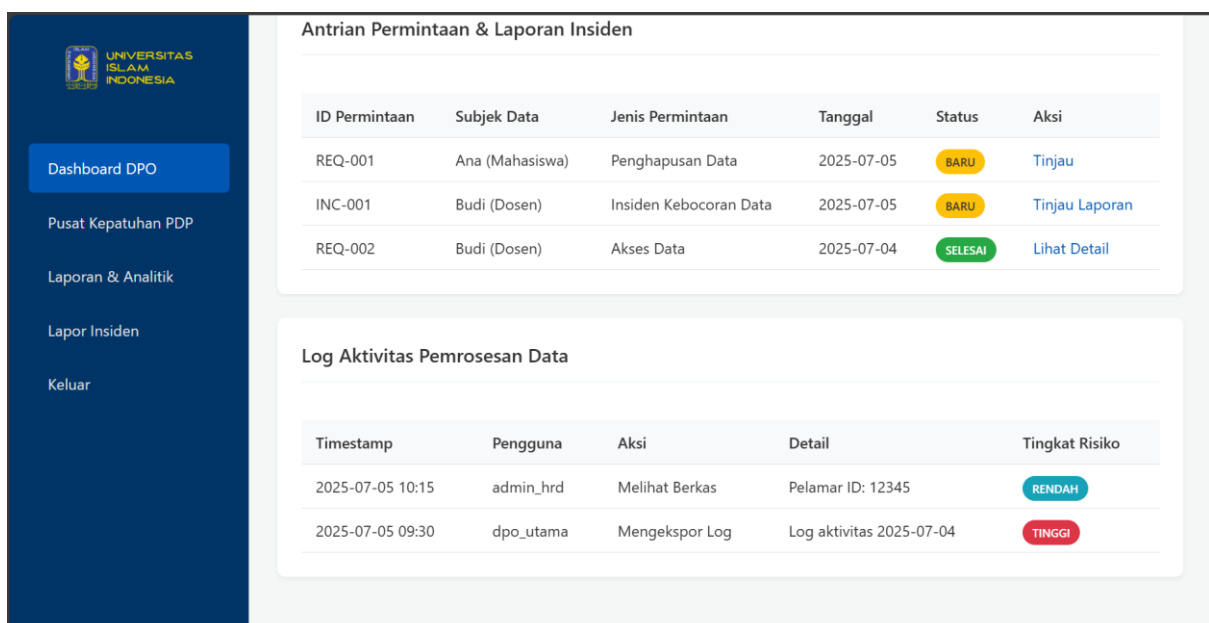
Pada fitur DPO atau *Data Protection Officer* ini dirancang untuk mendukung fungsi dan memastikan kepatuhan terhadap regulasi UU PDP. Didalam fitur DPO ditampilkan Dashboard yang berisi indikator-indikator mengenai sistem yang sudah disesuaikan terhadap UU PDP, serta terdapat Laporan dan Analitik yang membantu DPO melacak seluruh aktivitas sistem yang berhubungan dengan data pribadi.

A. Dashboard

Pada gambar 4.15 dan 4.16 memperlihatkan dashboard khusus Superadmin atau *Data Protection Officer* yang dilengkapi dengan indikator kepatuhan terhadap UU PDP seperti, daftar permintaan subjek data, serta log aktivitas data. Dengan fitur ini, sistem mendukung akuntabilitas dalam pengendalian data.



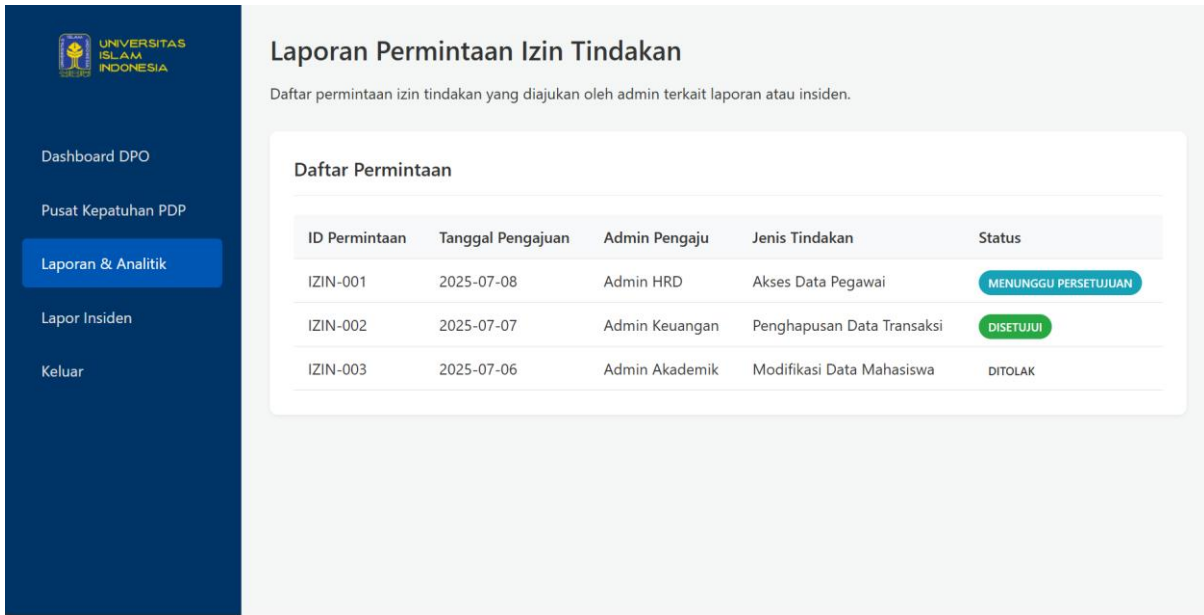
Gambar 4. 15 Dashboard DPO (1)



Gambar 4. 16 Dashboard DPO (2)

B. Laporan dan Analitik

Fitur ini dirancang untuk membantu DPO dalam melacak seluruh aktivitas sistem yang berhubungan dengan data pribadi, termasuk permintaan sistem akses hingga penghapusan data. Pada gambar 4.17 memperlihatkan tampilan visual indikator-indikator kepatuhan seperti status permintaan hak subjek data. Informasi ini disajikan untuk memudahkan DPO dalam melakukan evaluasi serta memastikan bahwa proses pemrosesan data pribadi dilakukan sesuai dengan prinsip-prinsip regulasi Undang-Undang Pelindungan Data Pribadi.



ID Permintaan	Tanggal Pengajuan	Admin Pengaju	Jenis Tindakan	Status
IZIN-001	2025-07-08	Admin HRD	Akses Data Pegawai	MENUNGGU PERSETUJUAN
IZIN-002	2025-07-07	Admin Keuangan	Penghapusan Data Transaksi	DISETUJUI
IZIN-003	2025-07-06	Admin Akademik	Modifikasi Data Mahasiswa	DITOLAK

Gambar 4. 17 Laporan dan Analitik

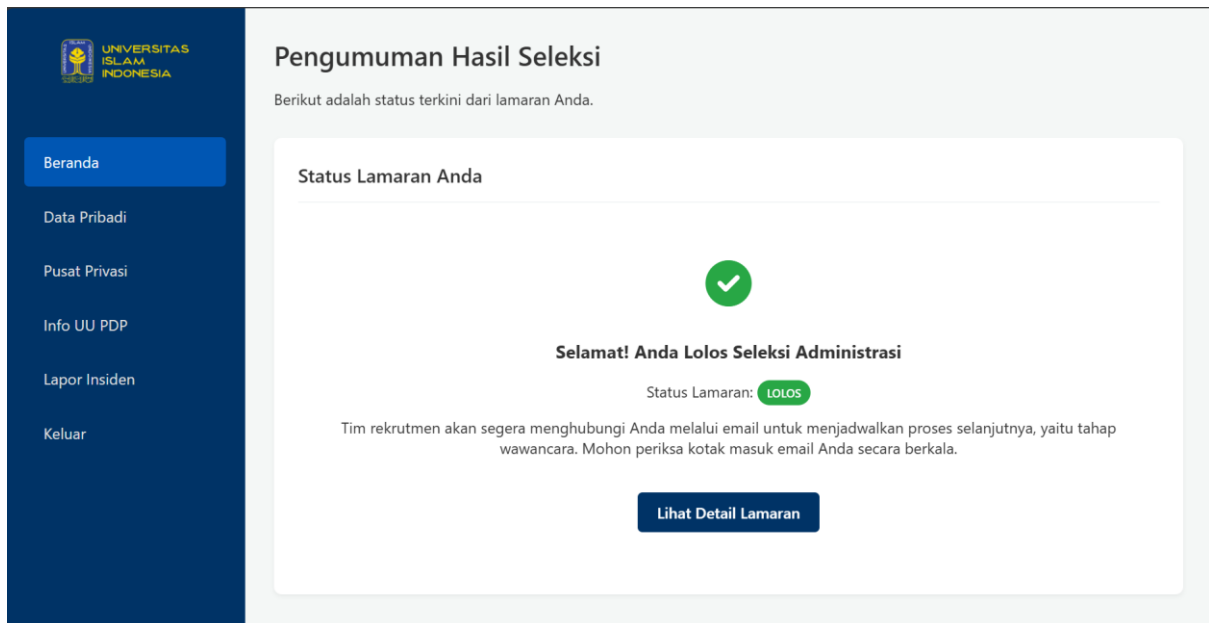
4.4.4 Fitur Pegawai

Pada fitur ini setiap pegawai seperti tenaga pendidikan dan dosen dapat mengelola dan memahami informasi data pribadinya sendiri. Terdapat *Dashboard* pegawai yang menampilkan status seleksi, seperti “lolos seleksi” atau “tidak lolos”. Lalu terdapat fitur Pusat Privasi yang memberikan akses untuk mengolah data para pegawai, seperti unduh data, edit profil, serta dapat mengajukan penghapusan data. Selanjutnya fitur *Pop-up* pembaruan data yang menampilkan notifikasi setelah adanya modifikasi pembaruan data yang dilakukan oleh pengendali data maupun pegawai. Setelah itu, terdapat informasi data pribadi di dalam fitur Data Pribadi untuk meninjau secara detail data pribadi pegawai yang tersimpan di sistem.

A. *Dashboard* Pegawai

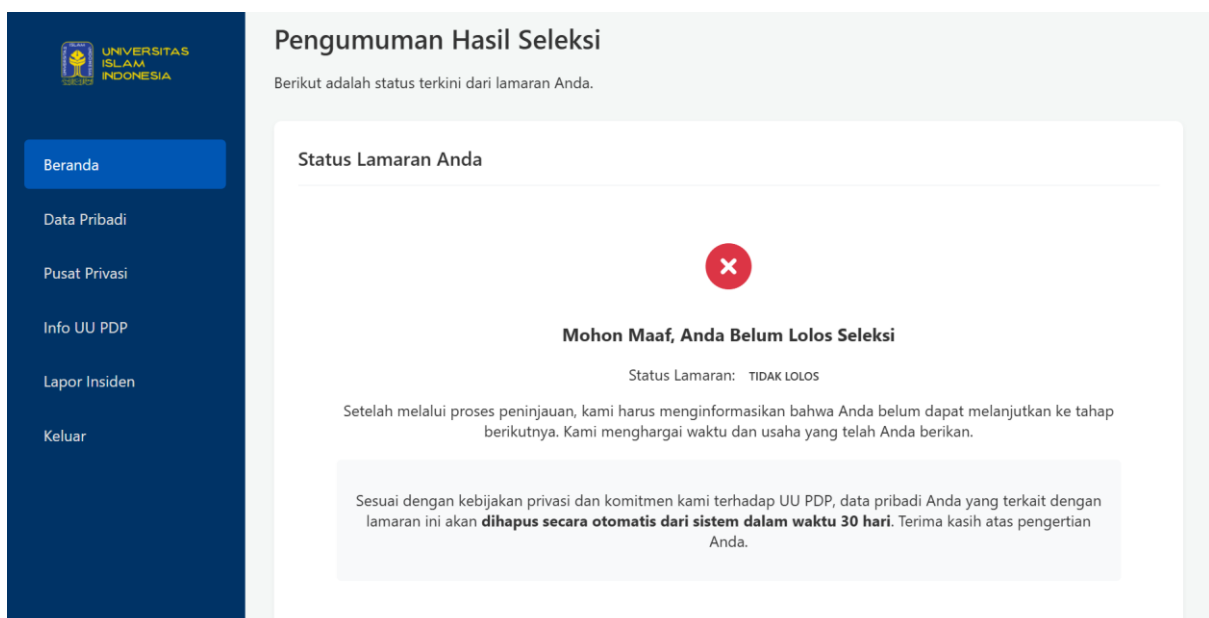
Dashboard pegawai menampilkan sistem antarmuka yang digunakan untuk menampilkan status seleksi, seperti “lolos seleksi” atau “tidak lolos”. Tampilan ini mencerminkan bagian dari sistem rekrutmen yang transparan, di mana pegawai dapat mengetahui hasil seleksi secara langsung melalui antarmuka sistem.

Pada Gambar 4.18 *Dashboard* Pegawai Lolos Seleksi menampilkan informasi detail bagi pelamar yang dinyatakan “LOLOS” waktu pengumuman, serta dapat melanjutkan ke langkah selanjutnya, seperti pengisian data personal. Hal ini memastikan pengguna agar mendapat kejelasan dan panduan sistematis setelah dinyatakan lolos.



Gambar 4. 18 Dashboard Pegawai Lolos Seleksi

Lalu pada Gambar 4.19 memberikan informasi ringkas dan menampilkan status kepada pelamar yang dinyatakan “TIDAK LOLOS” atau belum dapat melanjutkan ke tahap berikutnya, serta sistem juga akan memberikan informasi bahwa data akan dihapus secara otomatis sesuai ketentuan yang berlaku, sebagai bentuk implementasi Undang-Undang Pelindungan Data Pribadi.

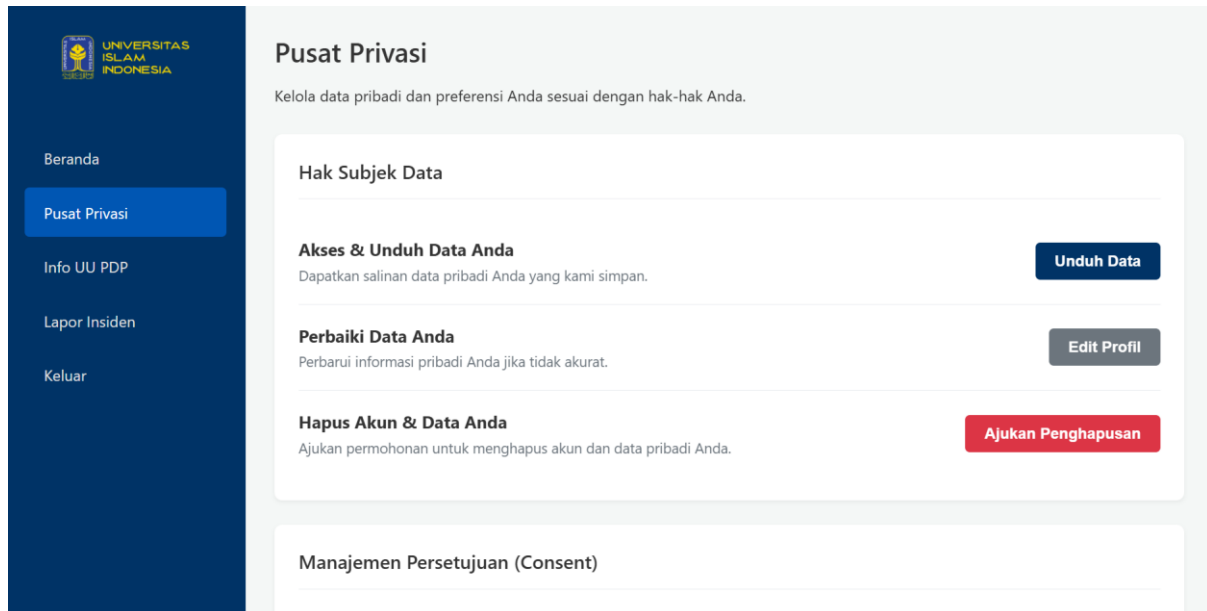


Gambar 4. 19 Dashboard Pegawai Tidak Lolos Seleksi

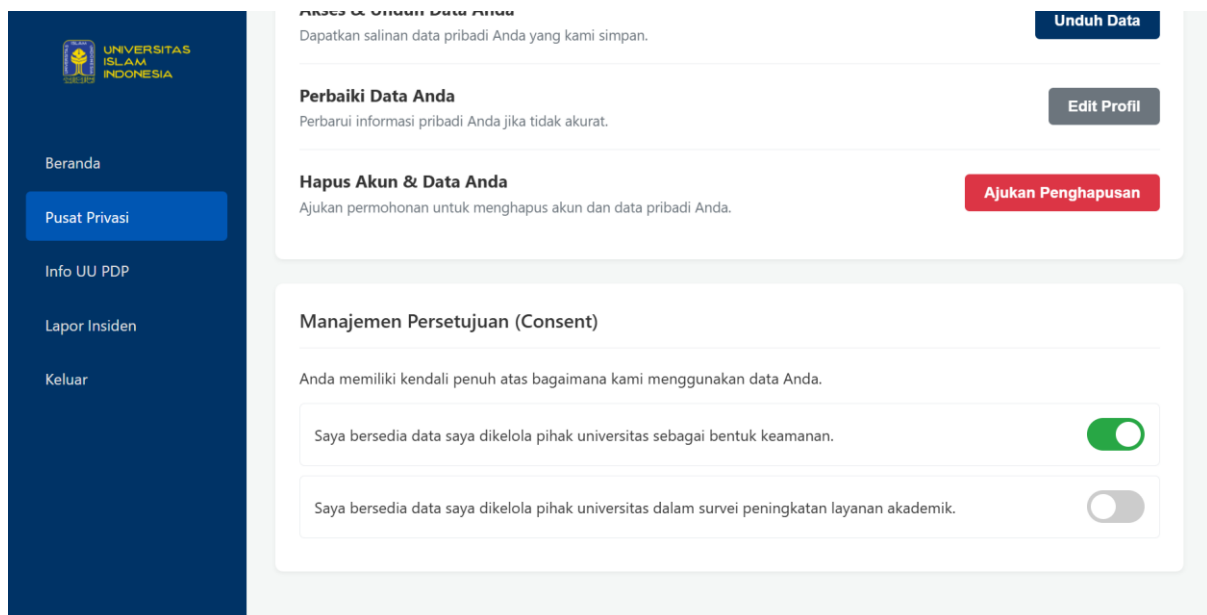
B. Pusat Privasi

Pada Gambar 4.20 dan Gambar 4.21 menunjukkan bahwa pengguna dapat mengelola hak akses datanya. Oleh karena itu di halaman ini tersedia fitur untuk mengunduh data,

memperbaiki data, dan mengajukan penghapusan akun dan data pribadi. Fitur ini memberi kontrol langsung kepada pengguna atas data mereka sesuai dengan prinsip di dalam Undang-Undang Pelindungan Data Pribadi.



Gambar 4. 20 Pusat Privasi (1)

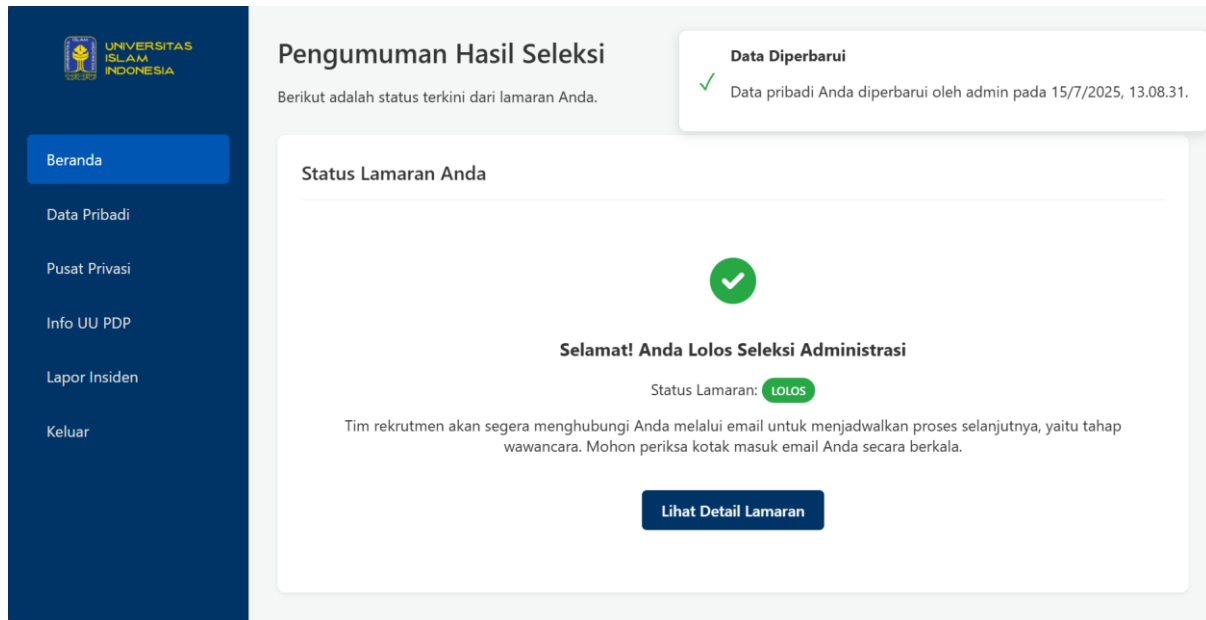


Gambar 4. 21 Pusat Privasi (2)

C. Pop-Up Pembaruan Data

Pada dashboard pegawai ditampilkan notifikasi saat data pribadi pengguna diperbarui oleh admin seperti pada Gambar 4.22. Notifikasi ini mencantumkan waktu dan memastikan aktivitas dalam sistem dilakukan dengan transparansi. Fungsi utama dari fitur ini adalah untuk menjamin bahwa setiap aktivitas terhadap data pribadi dilakukan secara transparan dan terinformasikan,

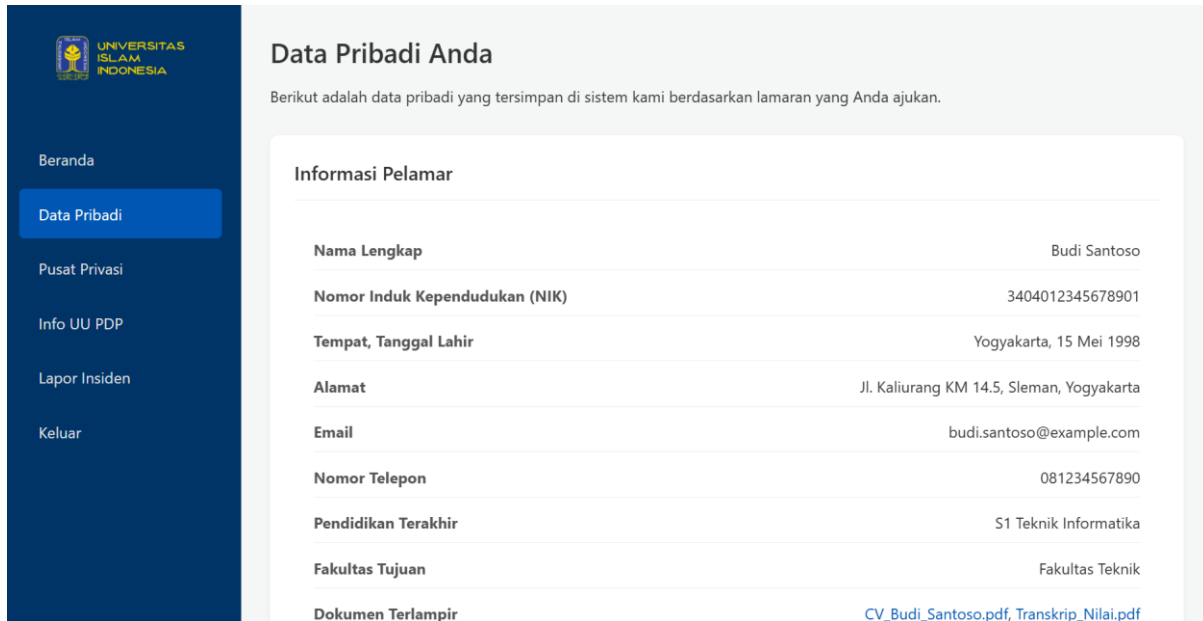
sesuai prinsip transparansi dan pemberitahuan dalam Pasal 30 ayat 2 Undang-Undang Pelindungan Data Pribadi (UU PDP) yang berbunyi “Pengendali Data Pribadi wajib memberitahukan hasil pembaruan dan/atau perbaikan data kepada Subjek Data Pribadi”.



Gambar 4. 22 Pop-up Pembaruan Data

D. Data Pribadi

Pada gambar 4.23 memperlihatkan data pribadi pengguna yang disimpan dan dikelola oleh sistem, yang berisi informasi sensitif seperti nama lengkap, NIK, tanggal lahir, alamat, nomor telepon, serta informasi administratif lainnya yang di input oleh pengguna dan tersimpan dalam sistem.



Data Pribadi Anda

Berikut adalah data pribadi yang tersimpan di sistem kami berdasarkan lamaran yang Anda ajukan.

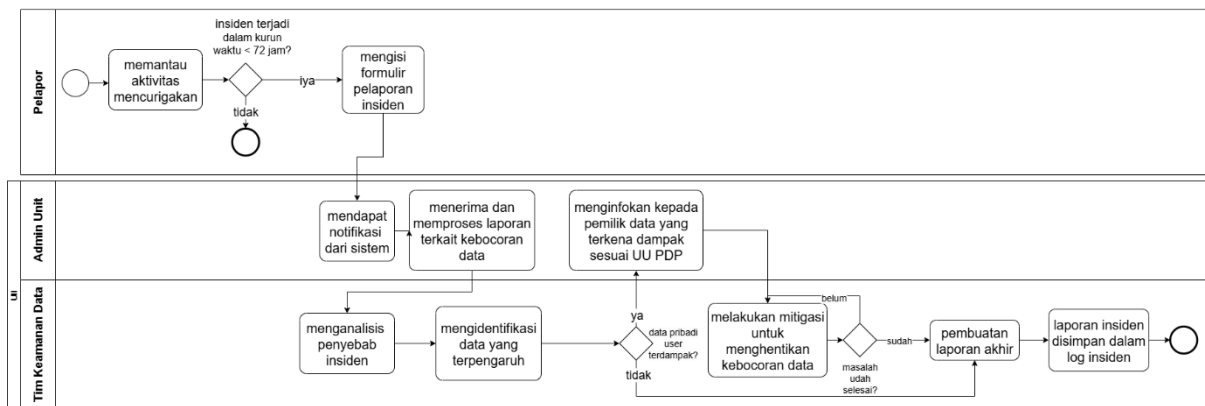
Informasi Pelamar	
Nama Lengkap	Budi Santoso
Nomor Induk Kependudukan (NIK)	3404012345678901
Tempat, Tanggal Lahir	Yogyakarta, 15 Mei 1998
Alamat	Jl. Kaliurang KM 14.5, Sleman, Yogyakarta
Email	budi.santoso@example.com
Nomor Telepon	081234567890
Pendidikan Terakhir	S1 Teknik Informatika
Fakultas Tujuan	Fakultas Teknik
Dokumen Terlampir	CV_Budi_Santoso.pdf , Transkrip_Nilai.pdf

Gambar 4. 23 Data Pribadi Pengguna

4.5 Evaluasi dan Validasi Model BPMN yang Diusulkan

Setelah perancangan model BPMN yang diusulkan dibuat, dilakukan evaluasi dan validasi untuk memastikan bahwa sistem yang diusulkan dapat dikembangkan sesuai dengan ketentuan yang ada dalam Undang-Undang Pelindungan Data Pribadi (UU PDP). Berdasarkan pengembangan model BPMN yang diusulkan, tidak dijelaskan bagaimana langkah para pengguna jika mengalami insiden kebocoran data. Oleh karena itu, terdapat improvisasi fitur untuk menyelaraskan dengan Pasal 46 ayat 1 Undang-Undang Pelindungan Data Pribadi yang berbunyi “Dalam hal terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 jam kepada Subjek Data Pribadi dan lembaga”, yaitu adanya fitur Pelaporan Kebocoran Data. Fitur ini berperan ketika pengguna mengalami aktivitas mencurigakan terkait kebocoran data. Telah dibuat model BPMN mengenai fitur Pelaporan Kebocoran Data yang dibuat menggunakan website *draw.io*.

PELAPORAN KEBOCORAN DATA



Gambar 4. 24 Diagram BPMN Pelaporan Kebocoran Data

Proses bisnis terkait fitur Pelaporan Kebocoran Data bisa dilihat pada Gambar 4.24. yang menampilkan tiga *lane* yang masing-masing terdiri dari Pelapor, Tim Keamanan Data, dan Admin Unit. Pelapor diartikan sebagai pihak yang memiliki hak melapor ketika terjadinya aktivitas mencurigakan terkait data pribadi pelapor. Kemudian Tim Keamanan Data berperan sebagai pihak yang berhak menganalisis penyebab, mengidentifikasi data yang terpengaruh, melakukan mitigasi untuk menghentikan setiap terjadinya kebocoran data, dan pembuatan laporan akhir serta menyimpan laporan insiden kedalam log insiden. Sedangkan Admin Unit berperan sebagai pihak yang menerima notifikasi dari sistem dan memproses laporan terkait kebocoran data, serta menginfokan kepada pemilik yang terkena dampak.

Mulanya Pelapor memantau aktivitas mencurigakan dalam kurun waktu kurang dari 72 jam. Jika aktivitas masih terjadi dalam kurun waktu kurang dari 72 jam pelapor dapat mengisi formulir pelaporan insiden. Lalu Admin Unit akan mendapatkan notifikasi dari sistem dan menerima serta memproses laporan terkait kebocoran data. Selanjutnya pihak Tim Keamanan Data menganalisis penyebab insiden kebocoran dan mengidentifikasi data yang terpengaruh. Jika Tim Keamanan Data tidak menemukan aktivitas mencurigakan dari data pelapor, tidak akan adanya tindakan lanjutan, sehingga Tim Keamanan Data akan membuat laporan akhir dan menyimpan laporan insiden ke dalam log insiden. Jika data pribadi pelapor terdampak, Admin Unit akan menginfokan kepada pemilik data yang terkena dampak, lalu Tim Keamanan Data melakukan mitigasi untuk menghentikan kebocoran data. Setelah mitigasi selesai Tim Keamanan Data akan membuat laporan akhir dan menyimpan laporan insiden ke dalam log insiden.

Gambar 4. 25 Lapori Insiden

Untuk memfasilitasi proses pelaporan kebocoran data, sistem menampilkan antarmuka yang bernama Lapori Insiden yang dapat diakses oleh pegawai dan admin unit. Pada gambar 4.25 yang menunjukkan di mana pegawai dan admin unit dapat mengisi informasi terkait insiden yang mereka alami atau amati. Halaman ini memberikan pilihan untuk menggambarkan jenis kebocoran data serta dapat disertakan bukti yang relevan untuk mendukung adanya indikasi kebocoran untuk memenuhi syarat laporan.

Dengan adanya fitur pelaporan ini, pegawai dan admin unit dapat lebih aktif berpartisipasi dalam menjaga keamanan data pribadi mereka dan melaporkan insiden yang dapat membahayakan privasi mereka. Proses ini juga akan meningkatkan transparansi dan pertanggungjawaban institusi dalam menangani insiden kebocoran data.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian mengenai penerapan Undang-Undang Pelindungan Data Pribadi (UU PDP) dalam manajemen risiko pengamanan informasi di institusi pendidikan tinggi, maka dapat disimpulkan hal-hal berikut:

1. Penerapan Undang-Undang Pelindungan Data Pribadi (UU PDP) dalam manajemen risiko pengamanan informasi di institusi pendidikan tinggi

Penerapan UU PDP di institusi belum memiliki kebijakan internal yang secara spesifik mengatur pelindungan data pribadi sesuai ketentuan UU PDP. Pengelolaan data cenderung bersifat administratif dan belum sepenuhnya didukung oleh sistem manajemen risiko yang terstruktur. Temuan ini menunjukkan bahwa masih terdapat kesenjangan antara regulasi dan implementasi teknis di lapangan, termasuk dalam aspek identifikasi risiko, mitigasi, dan evaluasi berkelanjutan.

2. Risiko yang dihadapi oleh institusi pendidikan tinggi jika tidak adanya manajemen risiko untuk melindungi data pribadi sesuai dengan UU PDP

Tidak adanya manajemen risiko yang memadai dalam pelindungan data pribadi berpotensi menimbulkan sejumlah risiko signifikan bagi institusi pendidikan tinggi, di antaranya: kebocoran data mahasiswa dan dosen, penyalahgunaan informasi oleh pihak tidak bertanggung jawab, hingga kerugian reputasi institusi. Selain itu, institusi juga terancam sanksi hukum dan administratif jika terbukti melanggar ketentuan UU PDP. Risiko-risiko ini menunjukkan urgensi bagi institusi pendidikan untuk segera membentuk kebijakan pelindungan data dan manajemen risiko yang terintegrasi, serta melakukan peningkatan kapasitas sumber daya manusia di bidang keamanan informasi.

5.2 Saran

Berdasarkan kesimpulan yang telah dipaparkan, peneliti memberikan beberapa saran sebagai berikut

1. Bagi institusi pendidikan tinggi

Disarankan agar institusi pendidikan tinggi segera menyusun dan menerapkan kebijakan internal terkait pelindungan data pribadi yang selaras dengan UU PDP.

Selain itu, Institusi perlu membangun sistem manajemen risiko pengamanan informasi yang komprehensif, termasuk pengawasan terhadap proses pengumpulan, penyimpanan, dan pemrosesan data pribadi civitas akademika.

2. Bagi pengelola teknologi informasi

Tim pengelola teknologi informasi di lingkungan kampus perlu diberikan pelatihan secara berkala mengenai regulasi UU PDP implementasi teknis keamanan informasi. Penguatan dalam hal enkripsi data, sistem otorisasi akses, dan deteksi dini kebocoran informasi menjadi prioritas utama untuk mengurangi risiko.

DAFTAR PUSTAKA

- Amine, A. M., Chakir, E. M., Issam, T., & Khamlichi, Y. I. (2023). A Review of Cybersecurity Management Standards Applied in Higher Education Institutions. *International Journal of Safety and Security Engineering*, 13(6), 1109–1116. <https://doi.org/10.18280/ijssse.130614>
- Arthaputri, S. F. A. (2024). Perlindungan Data Pribadi Sebagai Bentuk Perwujudan Cyber Security (Studi Komparatif Indonesia Dan Singapura). *Dinamika*, 30(1), 9495–9509.
- 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.
- Blessing, L. T. M., & Chakrabarti, A. (2009). DRM, a design research methodology. In *DRM, a Design Research Methodology*. Springer London. <https://doi.org/10.1007/978-1-84882-587-1>
- Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 04(02), 92–100. <https://doi.org/10.4236/jis.2013.42011>
- Fachri Yamin Universitas Janabadra Yogyakarta, A., Rachmawati Universitas Janabadra Yogyakarta, A., & Kevin Wijaya Universitas Janabadra Yogyakarta, J. (2024). PERLINDUNGAN DATA PRIBADI DALAM ERA DIGITAL: TANTANGAN DAN SOLUSI. In *Rio Aditia Pratama & Jonathan Kevin Wijaya Meraja Journal* (Vol. 7, Issue 2).
- Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: a perspective for higher education institutions. In *Journal of Computer Information Systems* (Vol. 60, Issue 3). <https://doi.org/10.1080/08874417.2018.1432996>
- Junaedi, Said, T. G., & Tahir, M. (2023). Criminal for Leaking Administs Data of PDDIKTI and PSD-PTU According to Law Number 19 Year 2016 Concerning ITE. *East Asian Journal of Multidisciplinary Research*, 2(2). <https://doi.org/10.55927/eajmr.v2i2.3026>
- 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>
- Lee, D. H., Kim, Y. S., Koh, Y. Y., Song, K. Y., & Chang, I. H. (2021). Forecasting COVID-19 confirmed cases using empirical data analysis in Korea. *Healthcare*, 9(3), 254.

- 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.
- Primaranti, J., Setyowardhani, A. F., Nurlela, I., Ghrandiaz, V., & Yulhendri, Y. (2023). Analisis Resiko Keamanan Informasi Website Repository Digital Library Menggunakan Framework ISO/IEC 27001 & 27002: Studi Kasus Perguruan tinggi X. *Jurnal Riset Multidisiplin Dan Inovasi Teknologi*, 2(01), 327–373. <https://doi.org/10.59653/jimat.v2i01.500>
- Ridei, N., Tytova, N., Liubarets, V., Katsero, O., & Bakhmat, N. (2021). Methodology of Safety and Quality of Life on the Basis of Noospheric Education System Formation. *Strategies for Policy in Science and Education-Strategii Na Obrazovatelnata i Nauchnata Politika*, 29(1). <https://doi.org/10.53656/str2021-1-6-meth>
- Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment. *Hasanuddin Law Review*, 10(1), 1–20.
- Simbolon, V. A., & Juwono, V. (2022). Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation. *Publik (Jurnal Ilmu Administrasi)*, 11(2), 178–190.
- Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata kelola perlindungan data pribadi di era metaverse (telaah yuridis undang-undang perlindungan data pribadi). *Masalah-Masalah Hukum*, 52(1), 97–106.
- Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *Innovative: Journal Of Social Science Research*, 3(2), 4208–4221.
- 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).
- Wibowo, A., Alawiyah, W., & Azriadi. (2024). The importance of personal data protection in Indonesia's economic development. *Cogent Social Sciences*, 10(1), 2306751.
- 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.

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

LAMPIRAN

UlllInsani
Admin Dashboard

Dashboard Admin

Manajemen Pegawai

Lapor Insiden

Keluar

Dashboard Admin

Kelola data pelamar, status seleksi, dan penugasan fakultas.

Daftar Pelamar

ID Pelamar	Nama	Fakultas Tujuan	Status Berkas	Aksi
PLMR-001	Budi Santoso	Fakultas Teknik	BARU	<div>SortirUbah Status</div>
PLMR-002	Siti Aminah	Fakultas Hukum	LOLOS BERKAS	<div>Buat NIUIinformasi Lanjut</div>
PLMR-003	Joko Susilo	Fakultas Ekonomi	TIDAK LOLOS	<div>Lihat Detail</div>

Penugasan Seleksi per Fakultas

Pilih Fakultas

UlllInsani

Beranda

Pusat Privasi

Info UU PDP

Keluar

Kewajiban Kami sebagai Pengendali Data Pribadi

Sebagai Pengendali Data, Universitas memiliki tanggung jawab yang besar. Berikut adalah kewajiban kami yang telah diimplementasikan ke dalam fitur di sistem UlllInsani:

- Memiliki Dasar Hukum Pemrosesan (Pasal 20):** Kami tidak akan memproses data Anda tanpa dasar hukum yang jelas, terutama persetujuan (consent) yang Anda berikan untuk setiap tujuan pemrosesan.
- Memberikan Informasi Transparan (Pasal 21):** Sebelum meminta persetujuan Anda, kami wajib menginformasikan mengenai legalitas, tujuan, jenis data, hingga jangka waktu penyimpanan data.
- Menjamin Akurasi Data (Pasal 29 & 30):** Kami harus memastikan bahwa data yang kami proses akurat dan lengkap. Jika ada permintaan perbaikan, kami wajib memprosesnya sesegera mungkin.
- Merekam Seluruh Kegiatan Pemrosesan (Pasal 31):** Seluruh aktivitas pemrosesan data di sistem ini kami catat (logging) untuk menunjukkan akuntabilitas kami.
- Menjamin Keamanan Data (Pasal 35 & 38):** Kami wajib melindungi data Anda dari akses tidak sah. Sistem UlllInsani telah dilengkapi dengan sistem keamanan teknis dan operasional untuk memastikan hal tersebut.
- Menjaga Kerahasiaan Data (Pasal 36):** Semua data pribadi yang kami kelola bersifat rahasia. Hanya pihak yang memiliki kewenangan yang dapat mengaksesnya.
- Memberitahukan Kegagalan Pelindungan Data (Pasal 46):** Jika terjadi insiden kebocoran data, kami wajib memberitahukannya kepada Anda dan lembaga terkait paling lambat dalam 3x24 jam.

Pada intinya, sistem UlllInsani ini dibangun tidak hanya untuk menjadi canggih, tetapi juga agar dapat diandalkan dan patuh terhadap hukum. Kepercayaan Anda adalah prioritas utama kami.

Selamat Datang

Silakan masuk untuk melanjutkan

Email

admin@admin.com

Password

....

Masuk

Dengan masuk, Anda menyetujui [Syarat & Ketentuan](#) dan [Kebijakan Privasi](#) kami.

Belum punya akun? [Daftar di sini](#)