



Analisis Kesesuaian Pengelolaan Data Biometrik Pemohon Paspor dalam Permenimipas Nomor 11 Tahun 2026 dengan Prinsip Pelindungan Data Pribadi

Rafael Rocco Hutahaean^{1*}, Pascalis Danny Kristi Wibowo², Anindito Rizki Wiraputra³

¹⁻³Hukum Keimigrasian, Politeknik Imigrasi dan Pemasarakatan, Indonesia

*Penulis Korespondensi: faelhutahaean@gmail.com

Abstract. *Biometric data of passport applicants, in the form of facial images and fingerprints, is classified as specific Personal Data under Article 4(2) of Law Number 27 of 2022 on Personal Data Protection (PDP Law), thereby demanding a stricter standard of protection. This study examines the conformity of biometric data management under Minister of Immigration and Correctional Affairs Regulation Number 11 of 2026 on Ordinary Passports and Travel Documents in Lieu of Passports (Permenimipas No. 11/2026) with the principles of the PDP Law, employing a normative-juridical method through statutory and conceptual approaches. The findings reveal partial and asymmetrical conformity: the regulation entirely omits provisions on appointing a Personal Data Protection Officer (PPDP), implementation of Data Protection Impact Assessment, data retention periods, technical security standards, and incident notification—a gap rendered more urgent following Constitutional Court Decision Number 151/PUU-XXII/2024 concerning the Judicial Review of Law Number 27 of 2022 concerning Personal Data Protection (Constitutional Court Decision No. 151/PUU-XXII/2024), which broadened the scope of the PPDP appointment obligation. This study recommends harmonizing immigration regulations with the PDP Law to ensure legal certainty for passport applicants as data subjects.*

Keywords. *Biometric Data; Data Protection Officer; Immigration Services; Legal Certainty; Personal Data Protection.*

Abstrak. Data biometrik pemohon paspor, berupa foto wajah dan sidik jari, tergolong Data Pribadi yang bersifat spesifik menurut Pasal 4 ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sehingga menuntut standar pelindungan yang lebih ketat. Penelitian ini mengkaji kesesuaian pengaturan pengelolaan data biometrik dalam Peraturan Menteri Imigrasi dan Pemasarakatan Nomor 11 Tahun 2026 tentang Paspor Biasa dan Surat Perjalanan Laksana Paspor (Permenimipas No. 11 Tahun 2026) dengan prinsip-prinsip UU PDP dengan menggunakan metode yuridis-normatif melalui pendekatan perundang-undangan dan konseptual. Hasil penelitian menunjukkan kesesuaian yang parsial dan tidak simetris: regulasi ini sama sekali belum mengatur penunjukan Pejabat Pelindungan Data Pribadi (PPDP), pelaksanaan Penilaian Dampak Pelindungan Data Pribadi, retensi data, standar keamanan teknis, maupun notifikasi insiden, suatu kesenjangan yang makin mendesak menyusul Putusan Mahkamah Konstitusi Nomor 151/PUU-XXII/2024 tentang Pengujian Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (Putusan MK No. 151/PUU-XXII/2024) yang memperluas cakupan kewajiban penunjukan PPDP. Penelitian ini merekomendasikan harmonisasi regulasi keimigrasian dengan UU PDP guna menjamin kepastian hukum bagi pemohon paspor selaku subjek data.

Kata kunci. Data Biometrik; Kepastian Hukum; Pejabat Pelindungan Data; Pelayanan Keimigrasian; Pelindungan Data Pribadi.

1. LATAR BELAKANG

Perkembangan teknologi informasi telah membawa perubahan mendasar dalam penyelenggaraan pelayanan publik, tidak terkecuali pada sektor keimigrasian. Transformasi digital ini diwujudkan melalui penerapan sistem paspor elektronik (*e-passport*) yang mengandalkan data biometrik berupa foto wajah dan sidik jari (daktiloskopi) (Sefrianti dkk., 2024). Data biometrik memiliki karakteristik yang unik dan melekat secara permanen pada diri seseorang sehingga penggunaannya sebagai alat identifikasi dinilai lebih akurat dan sulit dipalsukan dibandingkan dengan dokumen identitas konvensional (Sefrianti dkk., 2024).

Secara normatif, Pasal 1 angka 2 Permenimipas No. 11 Tahun 2026 mendefinisikan Paspor Republik Indonesia atau Paspor sebagai dokumen yang dikeluarkan oleh Pemerintah Republik Indonesia kepada warga Indonesia untuk melakukan perjalanan antarnegara yang berlaku selama jangka waktu tertentu. Sebagai identitas resmi yang diakui secara internasional, paspor tidak hanya berfungsi sebagai bukti kewarganegaraan, tetapi juga menjadi instrumen kontrol keimigrasian yang memuat data diri pemegangnya, termasuk data biometrik yang digunakan untuk keperluan verifikasi dan autentikasi identitas.

Tingginya kebutuhan masyarakat terhadap dokumen perjalanan ini tercermin dari volume penerbitan paspor yang tinggi setiap tahunnya. Data Direktorat Jenderal Imigrasi menunjukkan bahwa pada tahun 2025, tercatat 4.033.676 paspor berhasil diterbitkan (Direktorat Jenderal Imigrasi, 2026). Capaian tersebut menjadi faktor utama terwujudnya rekor Penerimaan Negara Bukan Pajak (PNBP) tertinggi sepanjang sejarah keimigrasian Indonesia, yaitu sebesar Rp10,4 triliun (Direktorat Jenderal Imigrasi, 2026). Tingginya angka permohonan ini turut dirasakan di berbagai kantor imigrasi daerah, salah satunya Kantor Imigrasi Kelas I Khusus TPI Ngurah Rai yang menghadapi tantangan signifikan akibat status Bali sebagai destinasi internasional utama sehingga menuntut ketersediaan layanan yang lebih cepat, transparan, dan akuntabel (Darmaputra & Prabawati, 2025).

Guna merespons tingginya volume permohonan tersebut sekaligus mendorong penerapan sistem paspor elektronik, Direktorat Jenderal Imigrasi meluncurkan aplikasi M-Paspor sebagai bentuk inovasi pelayanan publik berbasis *electronic government* (*e-government*). Aplikasi ini merupakan pengembangan dari sistem sebelumnya, yaitu Aplikasi Pendaftaran Antrean Paspor Online (APAPO) Imigrasi dengan menghadirkan fitur yang lebih lengkap dan ramah pengguna (Direktorat Jenderal Imigrasi, 2022). Melalui M-Paspor, pemohon dapat melakukan pendaftaran secara mandiri, mengunggah dokumen persyaratan, melakukan pembayaran biaya paspor di awal melalui berbagai kanal digital, memilih jadwal dan lokasi kedatangan, serta memantau status permohonan secara *real-time*, sebelum mendatangi kantor imigrasi untuk menjalani proses pengambilan foto wajah dan sidik jari secara langsung. Sistem ini juga terintegrasi dengan data kependudukan Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil) untuk validasi Nomor Induk Kependudukan secara otomatis, serta terhubung langsung dengan Sistem Informasi Manajemen Keimigrasian (SIMKIM) yang menjadi basis data utama dalam proses verifikasi dan adjudikasi data biometrik pemohon paspor (Darmaputra & Prabawati, 2025).

Efisiensi yang dihadirkan oleh aplikasi M-Paspor ini berdampak langsung pada pelayanan di Kantor Imigrasi Kelas I Khusus TPI Ngurah Rai. Penelitian yang dilakukan di

kantor tersebut menunjukkan bahwa digitalisasi melalui aplikasi M-Paspor secara signifikan mengurangi durasi tatap muka, meminimalisasi antrean di lokasi pelayanan, serta memperkuat aspek transparansi dan akuntabilitas layanan keimigrasian (Darmaputra & Prabawati, 2025). Hal serupa juga dirasakan di Kantor Imigrasi Kelas I Khusus TPI Batam. Kedudukan strategis Batam sebagai kota perdagangan bebas (*Free Trade Zone*) menjadikan Batam sebagai pusat perlintasan internasional di Provinsi Kepulauan Riau yang berdampak langsung pada melonjaknya angka pendaftaran paspor melalui M-Paspor (Lubis & Saraan, 2024).

Namun, lonjakan angka pendaftaran paspor via kanal digital tersebut berbanding lurus dengan pemrosesan data biometrik yang intens. Karakteristik data biometrik yang tidak dapat diubah (*immutable*) menjadikannya kategori data pribadi yang memiliki risiko penyalahgunaan dan dampak kerugian yang fatal apabila terjadi kebocoran atau pemrosesan yang tidak sah. Berbeda dengan kata sandi atau nomor identitas, data biometrik tidak dapat diganti atau diperbarui apabila telah disalahgunakan (Yeovandi dkk., 2025). Ketika jutaan data biometrik dihimpun, dipertukarkan, dan dikelola secara terpusat dalam Sistem Informasi Manajemen Keimigrasian (SIMKIM), timbul kerentanan teknis berupa kegagalan sistem serta risiko utama berupa kebocoran data (*data breach*) (Kumar dkk., 2025). Risiko pada basis data pemerintah yang tersentralisasi ini dibuktikan oleh insiden peretasan berskala masif terhadap sistem Office of Personnel Management di Amerika Serikat pada tahun 2015 yang membocorkan data jutaan pegawai federal (Mills & Harclerode, 2017). Berkaca dari insiden tersebut, perlindungan teknis yang ketat mutlak diperlukan karena sistem institusi negara merupakan target utama dari serangan siber.

Kesadaran terhadap risiko kebocoran data telah diakomodasi dalam Pasal 4 ayat (2) UU PDP yang secara tegas mengklasifikasikan data biometrik sebagai Data Pribadi yang bersifat spesifik; kategori yang sama dengan data kesehatan, data genetika, catatan kejahatan, data keuangan pribadi, dan data anak sehingga menuntut standar perlindungan yang lebih ketat dibandingkan dengan Data Pribadi yang bersifat umum. Konsekuensi normatif dari klasifikasi ini, antara lain, kewajiban tambahan bagi Pengendali Data Pribadi, seperti kewajiban penunjukan Pejabat Pelindungan Data Pribadi (PPDP), kejelasan mengenai jangka waktu retensi data, standar keamanan teknis yang memadai, serta mekanisme notifikasi kepada subjek data apabila terjadi kegagalan perlindungan data.

Di sisi lain, praktik pengumpulan dan pengelolaan data biometrik pemohon paspor, baik secara konvensional maupun melalui M-Paspor, diselenggarakan berdasarkan kerangka regulasi sektoral yang tidak secara khusus dirancang untuk mengakomodasi prinsip-prinsip UU PDP. Sejak 28 Juli 2026, ketentuan ini diatur dalam Permenimipas No. 11 Tahun 2026, yang

mencabut dan menggantikan Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 8 Tahun 2014 tentang Paspor Biasa dan Surat Perjalanan Laksana Paspor (Permenkumham No. 8 Tahun 2014) beserta perubahannya sebagai konsekuensi administratif perubahan nomenklatur kelembagaan pascapembentukan Kementerian Imigrasi dan Pemasarakatan melalui Peraturan Presiden Nomor 157 Tahun 2024 tentang Kementerian Imigrasi dan Pemasarakatan (Perpres No. 157 Tahun 2024), bukan sebagai pembaruan substansial terhadap mekanisme pengelolaan data biometrik (Lutfianingtyas, 2026). Ketentuan pengambilan foto dan sidik jari dalam Pasal 16 dan Pasal 21 Permenimipas No. 11 Tahun 2026 tetap mempertahankan substansi yang identik dengan regulasi sebelumnya, yaitu pencocokan data biometrik pemohon dengan basis data SIMKIM untuk keperluan verifikasi dan adjudikasi.

Momentum pembaruan regulasi secara menyeluruh ini, termasuk penggantian total atas Permenkumham No. 8 Tahun 2014, semestinya menjadi kesempatan strategis bagi pembentuk regulasi untuk melakukan harmonisasi antara ketentuan teknis keimigrasian dengan prinsip-prinsip yang diamanatkan UU PDP, mengingat kedua regulasi tersebut sama-sama mengatur objek yang tumpang tindih, yaitu pemrosesan data pribadi yang bersifat spesifik dalam skala nasional. Akan tetapi, pemeriksaan awal terhadap batang tubuh Permenimipas No. 11 Tahun 2026 menunjukkan bahwa regulasi ini tidak memuat satu pun ketentuan mengenai penunjukan PPDP, jangka waktu retensi data biometrik, standar keamanan teknis penyimpanan data, maupun kewajiban notifikasi kepada subjek data apabila terjadi kegagalan pelindungan data.

Kajian literatur terdahulu mengenai digitalisasi keimigrasian di Indonesia sejauh ini masih terfragmentasi ke dalam beberapa diskursus yang berdiri sendiri. Pada diskursus pertama, evaluasi terhadap aplikasi M-Paspor masih didominasi oleh tolok ukur efisiensi operasional dan kualitas pelayanan publik; misalnya, riset Darmaputra dan Prabawati (2025) berfokus pada simplifikasi administrasi dan pemangkasan waktu antrean fisik di Denpasar, sedangkan kajian Lubis dan Saraan (2024) membatasi tinjauannya pada akuntabilitas manajemen kuota dan ketepatan waktu pelayanan di Batam. Pada diskursus kedua, literatur yang secara khusus membahas kerentanan data biometrik lebih banyak mengambil sudut pandang teknis keamanan siber murni, seperti riset Yeovandi, dkk. (2025) yang mengevaluasi kerentanan *spoofing* pada autentikasi biometrik telepon pintar tanpa menyentuh aspek kepatuhan regulasi sektoral. Di sisi lain, pada diskursus hukum pelindungan data, kajian mengenai tata kelola pasca-pengesahan UU PDP, seperti yang diuraikan oleh Machmudi (2025), telah menyoroti ancaman dari kekosongan institusional akibat ketiadaan lembaga pengawas independen, tetapi analisis tersebut masih bersifat makro dan tidak membedah tata kelola data spesifik pada sektor layanan keimigrasian.

Berdasarkan penelusuran literatur yang dilakukan, belum ditemukan penelitian yang secara khusus menyatukan ketiga diskursus tersebut. Maka dari itu, kebaruan ilmiah (*novelty*) penelitian ini terletak pada penggeseran paradigma. Penelitian ini tidak lagi mengevaluasi M-Paspor dan SIMKIM sekadar sebagai alat efisiensi pelayanan, melainkan mengujinya secara dogmatis sebagai infrastruktur pengelola data spesifik berskala masif. Secara spesifik, penelitian ini menguji kepatuhan normatif regulasi sektoral terbaru, yakni Permenimipas No. 11 Tahun 2026, terhadap kerangka akuntabilitas UU PDP dengan mengintegrasikan implikasi hukum Putusan MK No. 151/PUU-XXII/2024.

Fokus pengujian ini menjadi krusial karena ketiadaan harmonisasi regulasi sektoral di atas telah menimbulkan persoalan hukum yang mendasar mengenai kesesuaian antara praktik pelayanan keimigrasian, baik dalam wujud konvensional maupun yang telah bertransformasi melalui sistem paspor elektronik, dengan prinsip-prinsip perlindungan data pribadi, khususnya terkait dengan pembatasan tujuan pemrosesan (*purpose limitation*), mekanisme persetujuan atau dasar pemrosesan yang sah, serta akuntabilitas Pengendali Data Pribadi. Ketiadaan harmonisasi regulasi ini berpotensi menimbulkan kekosongan hukum (*legal vacuum*) sekaligus ketidakpastian hukum bagi subjek data, terutama dalam hal terjadi penyalahgunaan atau kebocoran data biometrik yang bersifat permanen dan tidak dapat dipulihkan (Razmetaeva, 2017). Berdasarkan uraian tersebut, penelitian ini bertujuan untuk mengkaji secara mendalam kesesuaian antara pengaturan pengelolaan data biometrik pemohon paspor dalam Permenimipas No. 11 Tahun 2026 dengan prinsip-prinsip perlindungan data pribadi sebagaimana diamanatkan dalam UU PDP, guna memberikan kontribusi akademis bagi upaya harmonisasi regulasi keimigrasian di masa mendatang.

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian yuridis-normatif (*normative legal research*) untuk mengkaji kesesuaian norma hukum antara Permenimipas No. 11 Tahun 2026 dengan UU PDP sehingga yang menjadi objek kajian bukanlah perilaku atau praktik empiris di lapangan, melainkan konsistensi dan harmonisasi norma hukum itu sendiri sebagai suatu sistem. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*) guna menelaah konsep perlindungan Data Pribadi yang bersifat spesifik, pembatasan tujuan pemrosesan, serta kewajiban dan akuntabilitas Pengendali Data Pribadi.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer yang mencakup UUD NRI 1945, UU PDP, Undang-Undang Nomor 6 Tahun 2011 tentang

Keimigrasian (UU No. 6 Tahun 2011) beserta perubahannya, Peraturan Pemerintah Nomor 31 Tahun 2013 tentang Peraturan Pelaksanaan Undang-Undang Nomor 6 Tahun 2011 tentang Keimigrasian (PP Nomor 31 Tahun 2013) beserta perubahannya, Permenimipas No. 11 Tahun 2026, Permenkumham No. 8 Tahun 2014 beserta perubahannya, dan Perpres Nomor 157 Tahun 2024. Bahan hukum tersebut didukung oleh bahan hukum sekunder berupa literatur hukum, jurnal ilmiah, dan hasil penelitian terdahulu serta bahan hukum tersier berupa kamus hukum, kamus bahasa Indonesia, dan sumber daring kredibel sebagai penunjang interpretasi.

Bahan hukum dihimpun melalui studi kepustakaan (*library research*) atas basis data resmi peraturan perundang-undangan, yaitu JDIH Kementerian Imigrasi dan Pemasarakatan dan Berita Negara Republik Indonesia, serta basis data jurnal dan pangkalan data akademik. Analisis dilakukan secara kualitatif dengan metode preskriptif-analitis melalui empat tahap, yaitu identifikasi norma dalam Permenimipas No. 11 Tahun 2026 terkait pengumpulan, pengolahan, dan penyimpanan data biometrik; sinkronisasi horizontal dengan prinsip dan kewajiban normatif UU PDP untuk menemukan titik temu maupun titik kesenjangan; interpretasi sistematis dengan memperhatikan dasar hukum serta asas *lex superior derogat legi inferiori*; dan penarikan kesimpulan secara deduktif dari norma umum UU PDP terhadap norma khusus dalam Permenimipas No. 11 Tahun 2026.

3. HASIL DAN PEMBAHASAN

Klasifikasi Data Biometrik dalam Rezim Pelindungan Data Pribadi

Pasal 4 UU PDP membagi Data Pribadi ke dalam dua kategori, yaitu Data Pribadi yang bersifat umum dan Data Pribadi yang bersifat spesifik. Data biometrik didefinisikan sebagai data yang berkaitan dengan karakteristik fisik, fisiologis, atau perilaku individu yang memungkinkan identifikasi unik terhadapnya, termasuk gambar wajah dan data sidik jari (Republik Indonesia, 2022). Data ini dimasukkan secara tegas ke dalam kategori Data Pribadi yang bersifat spesifik, bersanding dengan data kesehatan, data genetika, catatan kejahatan, data anak, dan data keuangan pribadi. Penempatan ini bukan sekadar persoalan administratif, melainkan membawa konsekuensi normatif yang signifikan bagi seluruh proses pemrosesannya.

Data yang bersifat spesifik adalah data yang, apabila diproses secara tidak tepat, berpotensi menimbulkan dampak yang jauh lebih besar terhadap subjek data dibandingkan dengan data pribadi umum (Republik Indonesia, 2022). Dampak tersebut mencakup potensi diskriminasi dan kerugian yang bersifat permanen bagi pemiliknya. Karakteristik inilah yang membedakan data biometrik dari data identitas konvensional seperti nama atau alamat. Sidik

jari dan foto wajah yang direkam dalam proses permohonan paspor tidak dapat "diganti" apabila terjadi penyalahgunaan, sebagaimana kata sandi atau nomor rekening dapat diperbarui (Kumar dkk., 2025).

Konsekuensinya, standar perlindungan hukum yang dituntut terhadap pemrosesan data biometrik seharusnya lebih ketat dibandingkan dengan standar yang berlaku bagi data pribadi pada umumnya (Kumar dkk., 2025). Pemahaman terhadap klasifikasi ini menjadi kerangka acuan (*frame of reference*) bagi seluruh analisis berikutnya dalam penelitian ini. Setiap ketentuan dalam Permenimipas No. 11 Tahun 2026 yang bersinggungan dengan pengumpulan, penyimpanan, atau pemrosesan data biometrik pemohon paspor harus diuji terhadap standar perlindungan yang lebih tinggi ini, bukan terhadap standar minimal yang berlaku bagi data pribadi umum.

Dasar Hukum Pemrosesan Data Biometrik dalam Peraturan Pelayanan Paspor

Berpijak dari klasifikasi data pribadi yang digunakan di dalam paspor, langkah berikutnya adalah memetakan bagaimana Permenimipas No. 11 Tahun 2026 mengatur pengumpulan dan pemrosesan data biometrik pemohon paspor. Berdasarkan Pasal 16 ayat (1), penerbitan paspor biasa dilakukan melalui empat tahapan pokok, yaitu pemeriksaan kelengkapan dan keabsahan persyaratan, pembayaran biaya paspor, pengambilan foto dan sidik jari, serta wawancara. Ayat (2) melengkapi keempat tahapan tersebut dengan tahapan verifikasi dan adjudikasi. Ketentuan yang secara langsung menyentuh pemrosesan data biometrik termuat lebih spesifik dalam Pasal 21 ayat (2).

Pasal 21 ayat (2) menyatakan bahwa verifikasi dan adjudikasi dilakukan dengan mencocokkan data biometrik pemohon terhadap basis data yang tersimpan dalam SIMKIM. SIMKIM sendiri didefinisikan Pasal 1 angka 4 sebagai sistem teknologi informasi dan komunikasi yang digunakan untuk mengumpulkan, mengolah, dan menyajikan informasi. Sistem ini mendukung operasional, manajemen, dan pengambilan keputusan dalam melaksanakan fungsi keimigrasian secara menyeluruh.

Dari sisi legalitas dasar pemrosesan, praktik ini pada dasarnya tetap dapat dikategorikan sah menurut UU PDP. Pasal 20 ayat (2) UU PDP menyediakan enam dasar pemrosesan Data Pribadi yang sah, di antaranya pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai peraturan perundang-undangan, serta pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengendali Data Pribadi berdasarkan peraturan perundang-undangan. Ketentuan ini bermakna bahwa Pengendali Data Pribadi dapat memproses data tanpa persetujuan eksplisit subjek data, sepanjang terdapat kewajiban hukum atau pelaksanaan tugas kepentingan umum dan pelayanan publik yang mendasarinya. Maka

dari itu, pengambilan data biometrik pemohon paspor oleh Kementerian Imigrasi dan Pemasarakatan dapat dibenarkan secara hukum atas dasar kewajiban hukum (Pasal 20 ayat (2) huruf c UU PDP) sekaligus pelayanan publik (huruf e), tanpa harus bergantung pada mekanisme persetujuan tertulis eksplisit sebagaimana lazim berlaku di sektor komersial.

Meskipun demikian, perlu dicatat bahwa legalitas dasar pemrosesan hanyalah satu dari sekian banyak dimensi kepatuhan dalam UU PDP. Keabsahan dasar tersebut tidak serta-merta membebaskan Pengendali Data Pribadi dari kewajiban derivatif yang menyertainya, terutama saat memproses Data Pribadi spesifik dalam skala besar (Lutfianingtyas, 2025). Pada titik inilah kesesuaian antara Permenimipas No. 11 Tahun 2026 dan UU PDP mulai menunjukkan keretakan, sebagaimana akan diuraikan pada bagian selanjutnya.

3.3 Kesenjangan pada Kewajiban Derivatif Pengendali Data Pribadi

UU PDP membebaskan serangkaian kewajiban turunan kepada Pengendali Data Pribadi. Namun, tinjauan terhadap 81 pasal Permenimipas No. 11 Tahun 2026 menunjukkan absensi pengaturan krusial mengenai standar keamanan teknis, masa retensi data biometrik, kewajiban notifikasi kebocoran data, hingga penunjukan PPDP. Selain itu, tidak dicantumkannya UU PDP dalam bagian “Mengingat” menunjukkan bahwa keterkaitan regulasi ini dengan kerangka pelindungan data pribadi belum tercermin secara eksplisit dalam dasar hukum pembentukannya. Kondisi tersebut memperkuat temuan mengenai belum optimalnya integrasi norma UU PDP ke dalam pengaturan teknis keimigrasian.

Kekosongan Ekosistem Mitigasi Risiko: Standar Keamanan, Retensi, dan Notifikasi Insiden

Pelindungan data pribadi sejatinya merupakan manifestasi dari hak asasi manusia atas pelindungan diri pribadi yang dijamin secara konstitusional oleh Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945) (Sinaga & Putri, 2020). Guna memberikan kepastian dan keamanan atas hak fundamental tersebut, UU PDP membebaskan kewajiban positif kepada setiap pengendali data pribadi. Kewajiban umum ini secara kumulatif mencakup penerapan asas kerahasiaan dan prinsip keamanan, kepastian batas masa retensi pemrosesan, serta mitigasi risiko melalui kewajiban notifikasi insiden kebocoran data.

Dalam doktrin ilmu perundang-undangan, instrumen sektoral di tingkat kementerian memikul beban untuk menerjemahkan kerangka kewajiban umum tersebut ke dalam parameter operasional, termasuk dengan mendelegasikan kepatuhan teknisnya pada standar baku terotorisasi. Permenimipas No. 11 Tahun 2026 sejatinya telah mempraktikkan teknik pendelegasian keamanan ini, tetapi terbatas pada objek perlengkapan fisik paspor. Pasal 71

ayat (1) dan (2) regulasi tersebut secara eksplisit mewajibkan pemenuhan "spesifikasi teknis pengaman" untuk blangko paspor biasa, yang secara presisi dirujuk pada standarisasi International Civil Aviation Organization (ICAO). Akan tetapi, ketentuan sektoral yang setara untuk melindungi infrastruktur digital dan pangkalan data biometrik keimigrasian sama sekali belum ditemukan dalam batang tubuh regulasi tersebut.

Kekosongan pertama terletak pada absennya standar keamanan teknis (*security standard*). Dalam perkembangan hukum privasi global, standar keamanan teknis kini ditempatkan sebagai kewajiban hukum pengendali data (Rodrigues dkk., 2023). Yurisprudensi di Amerika Serikat menegaskan bahwa kegagalan pengendali data dalam menetapkan dan mematuhi standar keamanan teknis yang wajar bukanlah sekadar kelalaian operasional biasa, melainkan sebuah bentuk praktik yang tidak adil (*unfair practice*) yang melanggar pondasi perlindungan data (*FTC v. Wyndham Worldwide Corp.*, 2015). Mengingat sifat data biometrik yang unik, pengamanannya memerlukan metode kriptografi tingkat tinggi, seperti *homomorphic encryption*, yang membedakannya dari standar perlindungan data pribadi umum (Yang dkk., 2023). Tanpa adanya pendelegasian norma sektoral yang mewajibkan kepatuhan pada parameter teknis tertentu (seperti standar ISO atau pedoman Badan Siber dan Sandi Negara), instansi pengelola rentan terjebak pada pengamanan minimalis tanpa tolok ukur hukum yang jelas.

Kekosongan kedua menyangkut masa retensi data (*retention*). UU PDP secara tegas mensyaratkan penghapusan data setelah masa retensi pemrosesan berakhir sebagaimana diamanatkan Pasal 16, yang diperkuat oleh kewajiban transparansi informasi mengenai durasi retensi dalam Pasal 21. Akan tetapi, Permenimipas No. 11 Tahun 2026 tidak menetapkan durasi retensi data biometrik secara eksplisit. Tanpa kejelasan batas waktu, rekaman biometrik berpotensi disimpan tanpa batas waktu yang dapat diidentifikasi di dalam pangkalan data keimigrasian meskipun masa berlaku dokumen perjalanan telah habis.

Kekosongan ketiga bermuara pada ketiadaan mekanisme respons insiden (*incident response*). UU PDP melalui Pasal 46 telah membebaskan kewajiban pemberitahuan tertulis paling lambat 3x24 jam kepada subjek data apabila terjadi kegagalan perlindungan data. Namun, Permenimipas No. 11 Tahun 2026 tidak memberikan mekanisme operasional sektoral untuk mengimplementasikan instrumen notifikasi ini dalam konteks keimigrasian. Ketidadaan mekanisme operasional notifikasi insiden di dalam regulasi keimigrasian ini belum menerjemahkan hak fundamental warga negara atas transparansi. Mengingat rekaman biometrik tidak dapat direkayasa ulang atau diganti layaknya sebuah kata sandi saat diretas,

notifikasi dini merupakan jaring pengaman (*safety net*) yang tersisa bagi pemohon paspor untuk mewaspadai ancaman pencurian identitas lanjutan.

Berdasarkan penelusuran tersebut, persoalan yang terjadi sejatinya bukanlah bentuk kekosongan norma di level UU PDP, melainkan kegagalan atau ketidaklengkapan translasi norma umum UU PDP ke dalam tata kelola sektoral keimigrasian. Kegagalan Permenimipas No. 11 Tahun 2026 dalam mengadopsi standar keamanan infrastruktur digital, batas retensi, dan notifikasi insiden ini secara akumulatif menciptakan ekosistem yang rapuh, sehingga gagal memberikan kepastian hukum dan pelindungan privasi yang optimal bagi pemohon paspor.

Kewajiban Penunjukan PPDP dan Penilaian Dampak Pelindungan Data Pribadi Pasca-Putusan MK No. 151/PUU-XXII/2024

Kesenjangan pada aspek penunjukan PPDP menjadi makin signifikan menyusul terbitnya Putusan MK No. 151/PUU-XXII/2024. Sebelumnya, Pasal 53 ayat (1) UU PDP merumuskan tiga kriteria penunjukan PPDP secara kumulatif melalui penggunaan kata penghubung "dan". Penggunaan kata penghubung tersebut mengonstruksikan ketiga kriteria dalam huruf a, huruf b, dan huruf c sebagai persyaratan yang harus dipenuhi secara kumulatif agar kewajiban penunjukan PPDP timbul.

Dalam putusan yang diucapkan pada sidang pleno terbuka untuk umum pada 30 Juli 2025, Mahkamah Konstitusi mengabulkan permohonan pengujian materiil terhadap ketentuan ini. Mahkamah menilai bahwa ketiga kriteria dalam huruf a, huruf b, dan huruf c merupakan unsur yang bersifat independen dan masing-masing menggambarkan bentuk pemrosesan data pribadi yang berisiko tinggi (*high-risk data processing activities*). Menurut Mahkamah, konstruksi kumulatif tersebut dapat menyebabkan Pengendali Data Pribadi atau Prosesor Data Pribadi yang hanya memenuhi salah satu atau dua kriteria tidak memiliki kewajiban menunjuk PPDP, meskipun pemrosesan yang dilakukannya memiliki risiko tinggi terhadap pelindungan Data Pribadi. Mahkamah menilai keadaan ini tidak memberikan jaminan perlindungan hak atas diri pribadi sebagaimana dijamin Pasal 28G ayat (1) UUD NRI 1945. Atas pertimbangan tersebut, amar Putusan MK No. 151/PUU-XXII/2024 menyatakan kata "dan" dalam Pasal 53 ayat (1) huruf b UU PDP bertentangan dengan UUD NRI 1945 dan tidak mempunyai kekuatan hukum mengikat secara bersyarat, sepanjang tidak dimaknai "dan/atau" (Mahkamah Konstitusi Republik Indonesia, 2025).

Dalam konteks pemrosesan data biometrik pemohon paspor oleh Kementerian Imigrasi dan Pemasarakatan, setidaknya terdapat karakteristik pemrosesan yang relevan dengan kriteria penunjukan PPDP, yaitu pemrosesan untuk kepentingan pelayanan publik serta pemrosesan Data Pribadi yang bersifat spesifik dalam skala besar. Dengan berlakunya

pemaknaan “dan/atau” berdasarkan Putusan MK No. 151/PUU-XXII/2024, kewajiban penunjukan PPDP tidak lagi bergantung pada terpenuhinya seluruh kriteria secara kumulatif. Oleh karena itu, ketiadaan pengaturan mengenai penunjukan PPDP dalam Permenimipas No. 11 Tahun 2026 menunjukkan adanya kesenjangan antara kewajiban yang ditetapkan UU PDP sebagaimana telah dimaknai oleh Mahkamah Konstitusi dan pengaturan sektoral keimigrasian.

Kewajiban penunjukan PPDP tersebut berkaitan erat dengan kewajiban lain yang lahir dari karakteristik pemrosesan yang sama, yaitu Penilaian Dampak Pelindungan Data Pribadi (*Data Protection Impact Assessment* atau DPIA). DPIA merupakan proses sistematis untuk mengevaluasi potensi dampak suatu kegiatan pemrosesan terhadap privasi dan pelindungan Data Pribadi, sekaligus mengidentifikasi serta menentukan langkah yang diperlukan untuk mencegah, mengurangi, atau mengendalikan risiko yang ditimbulkannya (Yordanov, 2017). Dalam konteks pemrosesan data biometrik melalui sistem keimigrasian seperti SIMKIM dan M-Paspor, penilaian tersebut menjadi penting karena karakteristik dan konfigurasi sistem dapat mengalami perubahan seiring dengan pengembangan layanan, integrasi sistem, maupun perubahan teknologi yang digunakan (Yordanov, 2017). Oleh karena itu, hasil penilaian dampak perlu menjadi bagian dari tata kelola risiko yang dapat ditinjau kembali ketika terdapat perubahan dalam kegiatan pemrosesan yang berpotensi mengubah tingkat risiko terhadap Subjek Data Pribadi.

Pasal 34 ayat (1) UU PDP telah mewajibkan Pengendali Data Pribadi melakukan penilaian dampak apabila pemrosesan Data Pribadi memiliki potensi risiko tinggi terhadap Subjek Data Pribadi. Adapun Pasal 34 ayat (2) menetapkan sejumlah keadaan yang menunjukkan adanya potensi risiko tinggi, termasuk pemrosesan Data Pribadi yang bersifat spesifik dan pemrosesan Data Pribadi dalam skala besar. Dengan demikian, karakteristik pemrosesan data biometrik pemohon paspor yang telah memenuhi kriteria tersebut tidak hanya menimbulkan kewajiban penunjukan PPDP sebagaimana Pasal 53 UU PDP, tetapi juga secara langsung memicu kewajiban Pengendali Data Pribadi untuk melakukan DPIA berdasarkan Pasal 34 UU PDP.

Meskipun demikian, Permenimipas No. 11 Tahun 2026 tidak memuat mekanisme pelaksanaan DPIA dalam penyelenggaraan pemrosesan Data Pribadi pada sistem keimigrasian, termasuk mengenai prosedur identifikasi risiko, penilaian dampak, maupun langkah mitigasi yang harus dilakukan oleh Pengendali Data Pribadi. Ketidadaan mekanisme tersebut menunjukkan adanya kesenjangan antara kewajiban penilaian dampak yang telah ditetapkan secara langsung oleh Pasal 34 UU PDP dan pengaturan sektoral keimigrasian yang menjadi dasar operasional pemrosesan data biometrik. Dengan demikian, pengaturan sektoral perlu

menerjemahkan kewajiban DPIA ke dalam mekanisme tata kelola yang konkret agar penilaian risiko terhadap pemrosesan data biometrik tidak berhenti pada kewajiban normatif, tetapi menjadi bagian dari pengendalian risiko dalam penyelenggaraan sistem keimigrasian.

Keterbatasan Pemenuhan Hak Subjek Data

Sebagai pilar utama dalam rezim pelindungan data, UU PDP menjamin hak fundamental subjek data untuk melengkapi, memperbarui, dan memperbaiki ketidakakuratan data pribadi mereka (Republik Indonesia, 2022). Implementasi dari hak ini sejatinya telah diakomodasi secara parsial oleh Permenimipas No. 11 Tahun 2026 melalui mekanisme perubahan data identitas diri pemegang paspor sebagaimana diatur dalam Pasal 37 ayat (4) huruf c dan dijabarkan lebih lanjut dalam Pasal 38. Akan tetapi, cakupan koreksi ini terbatas pada data identitas umum dan sama sekali tidak menjangkau perbaikan atas inakurasi data biometrik. Padahal, potensi kerugian akibat inakurasi data biometrik jauh lebih fatal dibandingkan kekeliruan pada data identitas umum (Rodrigues dkk., 2023).

Ketiadaan mekanisme ini diduga berakar pada miskonsepsi yang menyamakan koreksi data biometrik dengan pembaruan karakteristik biometrik yang secara ilmiah memang bersifat *immutable*. Pada hakikatnya, terdapat pemisahan konseptual antara karakteristik biometrik dengan data biometrik. Wajah dan sidik jari merupakan wujud karakteristik biometrik, sementara data biometrik adalah wujud rekaman digital atas karakteristik tersebut (Jasserand, 2016). Dengan demikian, sekalipun karakteristik biometrik tidak dapat direkayasa, perbaikan terhadap data biometriknya tetap dapat dilakukan.

Dalam tata kelola data digital keimigrasian, perbaikan ini seharusnya diwujudkan melalui pemenuhan hak atas koreksi data (*right to rectification*), yaitu berupa hak perekaman ulang (*re-enrollment*) atau pembersihan distorsi pada sistem. Distorsi ini sangat rentan terjadi akibat kendala operasional, seperti kualitas tangkapan gambar yang buram (*noise*), malafungsi pada perangkat pemindai daktiloskopi, atau anomali saat pengikatan identitas digital ke dalam sistem (Kumar dkk., 2025). Sebagai contoh, distorsi sidik jari kerap terjadi pada sistem kontrol perbatasan (*border control*) akibat penempatan jari yang tidak tepat pada sensor, sehingga memicu kegagalan verifikasi berulang kali (Gu dkk., 2018).

Realitas operasional infrastruktur keimigrasian global menunjukkan bahwa tingkat kesalahan penolakan (*false reject rate*) akibat anomali teknis dan nonteknis masih sangat tinggi. Rata-rata satu dari sepuluh pengguna paspor yang sah gagal diverifikasi oleh mesin dan kehilangan akses perlintasan otomatis (Eastwood dkk., 2016). Kegagalan semacam ini acapkali tidak berkaitan dengan ancaman keamanan, tetapi murni merupakan malafungsi sistem (Eastwood dkk., 2016). Tanpa adanya pengakuan atas mekanisme *rectification*, Permenimipas

No. 11 Tahun 2026 belum menyediakan mekanisme yang secara eksplisit memungkinkan Subjek Data Pribadi untuk memastikan akurasi data spesifiknya. Akibatnya, Subjek Data Pribadi berisiko menanggung beban kerugian akibat kegagalan teknis infrastruktur, misalnya kegagalan sistem *border control*, secara sepihak.

Interpretasi Sistematis atas Kesenjangan Regulasi

Temuan mengenai kesenjangan kewajiban derivatif sebelumnya perlu ditempatkan dalam kerangka penafsiran sistem hukum secara keseluruhan, bukan sekadar dipahami sebagai daftar kekurangan yang berdiri sendiri. Dalam konteks hubungan antara UU PDP dan Permenimipas No. 11 Tahun 2026, penerapan *asas lex superior derogat legi inferiori* diperlukan untuk menentukan kedudukan serta batas keberlakuan masing-masing regulasi. Asas tersebut pada dasarnya menempatkan peraturan yang lebih tinggi sebagai rujukan yang harus didahulukan apabila terdapat pertentangan dengan peraturan yang lebih rendah. Dengan demikian, peraturan yang lebih rendah tidak dapat menyimpangi ketentuan yang ditetapkan oleh peraturan yang lebih tinggi (Eckhoff, 1975).

Dalam konteks ini, UU PDP berkedudukan sebagai undang-undang, sedangkan Permenimipas No. 11 Tahun 2026 merupakan peraturan menteri yang secara hierarkis berada di bawah undang-undang (Republik Indonesia, 2011a). Oleh karena itu, pengaturan teknis dalam Permenimipas No. 11 Tahun 2026 harus ditafsirkan dan diterapkan dalam kerangka kewajiban perlindungan Data Pribadi yang ditetapkan dalam UU PDP. Kedudukan Permenimipas sebagai peraturan teknis sektoral tidak memberikan dasar untuk mengesampingkan kewajiban yang telah ditetapkan pada tingkat undang-undang. Sepanjang penyelenggaraan keimigrasian melibatkan pengumpulan, penggunaan, penyimpanan, dan bentuk pemrosesan Data Pribadi lainnya, termasuk Data Pribadi yang bersifat spesifik, pemrosesan tersebut tetap harus memenuhi prinsip dan kewajiban yang ditentukan dalam UU PDP.

Penerapan asas hierarki tersebut tidak berarti bahwa terdapat pertentangan norma yang menyebabkan Permenimipas No. 11 Tahun 2026 harus dikesampingkan. Permenimipas tetap berlaku sebagai regulasi teknis operasional dalam penyelenggaraan keimigrasian. Permasalahannya terletak pada belum lengkapnya penerjemahan kewajiban UU PDP ke dalam pengaturan sektoral. Ketidadaan ketentuan mengenai penunjukan PPDP, mekanisme DPIA, retensi data biometrik, standar keamanan teknis, dan mekanisme sektoral terkait notifikasi insiden tidak menghapus kewajiban yang telah ditentukan oleh UU PDP. Sebaliknya, kondisi tersebut menunjukkan adanya kesenjangan pada tingkat regulasi teknis karena kewajiban yang

telah ditetapkan dalam UU PDP belum seluruhnya diterjemahkan ke dalam mekanisme penyelenggaraan keimigrasian.

Dengan demikian, hubungan antara UU PDP dan Permenimipas No. 11 Tahun 2026 lebih tepat dipahami sebagai hubungan antara norma umum pelindungan Data Pribadi dan pengaturan sektoral keimigrasian. UU PDP menetapkan prinsip, hak, serta kewajiban yang berlaku terhadap pemrosesan Data Pribadi, sedangkan Permenimipas mengatur penyelenggaraan paspor sebagai bagian dari kegiatan keimigrasian. Ketika pengaturan sektoral tersebut melibatkan pemrosesan Data Pribadi yang bersifat spesifik, ketentuan dalam Permenimipas harus dibaca secara sistematis dalam kerangka UU PDP. Dengan cara demikian, keberlakuan Permenimipas sebagai regulasi sektoral tetap dipertahankan tanpa mengurangi kewajiban pelindungan Data Pribadi yang bersumber dari UU PDP.

Kebutuhan untuk memperkuat hubungan tersebut semakin relevan karena pembaruan regulasi keimigrasian pada tahun 2026 merupakan momentum untuk melakukan harmonisasi pengaturan sektoral dengan perkembangan kerangka hukum pelindungan Data Pribadi. Harmonisasi diperlukan untuk memastikan bahwa berbagai peraturan perundang-undangan yang mengatur bidang yang saling berkaitan dapat berjalan secara konsisten dan tidak menimbulkan kesenjangan dalam penerapannya (Surya & Wahab, 2023). Dalam konteks penyelenggaraan paspor, pembaruan Permenimipas No. 11 Tahun 2026 seharusnya tidak hanya memperbarui aspek administratif dan teknis penyelenggaraan paspor, tetapi juga mengintegrasikan kewajiban pelindungan Data Pribadi yang relevan dengan pemrosesan data biometrik.

Kondisi tersebut menjadi semakin penting setelah Putusan MK No. 151/PUU-XXII/2024 memperluas cakupan kewajiban penunjukan PPDP sebagaimana telah diuraikan pada subbab sebelumnya. Pemrosesan data biometrik pemohon paspor yang bersifat spesifik dan dilakukan dalam skala besar menempatkan penyelenggaraan layanan keimigrasian dalam lingkup tata kelola pemrosesan Data Pribadi yang memerlukan akuntabilitas lebih kuat. Oleh karena itu, pengaturan sektoral perlu memberikan mekanisme yang jelas untuk menerjemahkan kewajiban tersebut ke dalam praktik penyelenggaraan layanan keimigrasian.

Dengan demikian, kesenjangan yang ditemukan dalam penelitian ini tidak menunjukkan bahwa Permenimipas No. 11 Tahun 2026 kehilangan keberlakuannya sebagai regulasi teknis keimigrasian. Persoalannya terletak pada belum sepenuhnya terintegrasinya standar pelindungan Data Pribadi ke dalam pengaturan teknis penyelenggaraan paspor. Dalam *perspektif lex superior derogat legi inferiori*, kewajiban yang ditetapkan UU PDP tetap mengikat penyelenggaraan keimigrasian, sedangkan Permenimipas No. 11 Tahun 2026

semestinya ditafsirkan dan diterapkan selaras dengan kewajiban tersebut. Oleh karena itu, kebutuhan yang muncul bukan pengesampingan salah satu regulasi, melainkan harmonisasi pengaturan teknis keimigrasian dengan kewajiban perlindungan Data Pribadi yang telah ditetapkan dalam UU PDP.

1. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan analisis yang telah diuraikan, dapat disimpulkan bahwa kesesuaian antara Permenimipas No. 11 Tahun 2026 dengan prinsip-prinsip perlindungan data pribadi dalam UU PDP bersifat parsial dan tidak simetris, sebagaimana dipetakan pada tiga tataran analisis berikut: (a) Pada tataran legalitas dasar pemrosesan, praktik pengumpulan data biometrik pemohon paspor telah sesuai dengan Pasal 20 ayat (2) UU PDP. Kesesuaian ini bersandar pada basis kewajiban hukum dan pelayanan publik yang sah. Pada titik ini, penelitian tidak menemukan persoalan mengenai dasar legalitas pemrosesan berdasarkan Pasal 20 ayat (2) UU PDP; (b) Pada tataran hak subjek data, terdapat pemenuhan yang bersifat sesuai sebagian melalui mekanisme perubahan data identitas pada Pasal 37 dan 38 Permenimipas No. 11 Tahun 2026. Cakupannya, baik secara sengaja maupun tidak sengaja, mengecualikan data biometrik itu sendiri. Padahal data biometrik justru merupakan kategori data yang paling membutuhkan mekanisme koreksi dan akuntabilitas yang jelas, mengingat sifatnya yang permanen dan tidak dapat diperbarui; serta (c) Pada tataran kewajiban derivatif sebagai Pengendali Data Pribadi, meliputi penunjukan PPDP, kejelasan masa retensi, standar keamanan teknis, dan kewajiban notifikasi insiden, regulasi teknis keimigrasian yang berlaku saat ini belum melakukan penyesuaian sama sekali. Kesenjangan pada tataran ini kini menjadi semakin sulit dipertahankan secara hukum menyusul Putusan MK Nomor 151/PUU-XXII/2024, yang telah dilewati ambang batasnya oleh fungsi keimigrasian bahkan sebelum putusan tersebut diucapkan.

Makin jauh suatu kewajiban dari sekadar keabsahan formal memproses data menuju akuntabilitas struktural sebagai pengelola data berskala besar, makin lebar pula kesenjangan antara norma yang diidealkan UU PDP dan norma yang senyatanya diatur dalam Permenimipas No. 11 Tahun 2026. Persoalan mendasarnya bukan terletak pada legitimasi Kementerian Imigrasi dan Pemasarakatan untuk mengumpulkan data biometrik pemohon paspor, melainkan pada ketiadaan kerangka akuntabilitas dan tata kelola risiko yang semestinya menyertai kewenangan tersebut ketika dijalankan terhadap kategori data yang paling rentan disalahgunakan. Terbitnya Putusan MK Nomor 151/PUU-XXII/2024 semakin mempertegas urgensi harmonisasi ini.

Berdasarkan simpulan tersebut, penelitian ini merekomendasikan agar Kementerian Imigrasi dan Pemasarakatan segera melakukan harmonisasi regulasi teknis keimigrasian dengan UU PDP, antara lain melalui pembentukan peraturan turunan atau pedoman teknis yang secara eksplisit: (a) mewajibkan pembentukan struktur Pejabat Pelindungan Data Pribadi (PPDP) secara berjenjang, mulai dari tingkat Direktorat Jenderal Imigrasi hingga unit pelaksana teknis di Kantor Imigrasi, sesuai dengan perluasan makna pada Putusan MK Nomor 151/PUU-XXII/2024; (b) merumuskan standar keamanan teknis minimum bagi penyimpanan dan pertukaran data biometrik di dalam ekosistem digital keimigrasian; (c) menetapkan standardisasi masa retensi data biometrik di dalam SIMKIM secara limitatif, dengan merumuskan pemisahan yang tegas antara masa retensi aktif (untuk operasional pelayanan dan perlintasan) dan masa retensi arsip (pasca-kedaluwarsanya paspor); (d) mewajibkan pelaksanaan DPIA secara periodik guna memitigasi risiko privasi, khususnya terhadap setiap rencana pengembangan arsitektur pangkalan data atau integrasi fitur baru pada SIMKIM dan aplikasi M-Paspor; dan (e) mengatur mekanisme operasional berupa Standar Operasional Prosedur (SOP) respons insiden kebocoran data, yang secara imperatif memuat kewajiban notifikasi tertulis kepada subjek data selambat-lambatnya 3x24 jam sejak kegagalan pelindungan data diketahui.

DAFTAR REFERENSI

- Asshiddiqie, J. (2010). Perihal undang-undang. Rajawali Pers.
- Darmaputra, K. I., & Prabawati, N. P. A. (2025). Optimalisasi layanan M-Paspor sebagai inovasi e-government dalam meningkatkan efektivitas pelayanan keimigrasian di Kantor Imigrasi Kelas I TPI Denpasar. *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial*, 2(12), 147–155.
- Direktorat Jenderal Imigrasi. (2022, 23 Januari). Aplikasi M-Paspor siap digunakan di seluruh Indonesia mulai 27 Januari 2022. Berita Direktorat Jenderal Imigrasi. Diakses 26 Juni 2026, dari <https://www.imigrasi.go.id/berita/2022/01/23/aplikasi-m-paspor-siap-digunakan-di-seluruh-indonesia-mulai-27-januari-2022?lang=id-ID>
- Direktorat Jenderal Imigrasi. (2026, 2 April). Imigrasi di era Yuldi Yusman: Rekor PNPB dan penguatan penegakan hukum [Siaran pers]. Diakses 25 Juni 2026, dari https://www.imigrasi.go.id/siaran_pers/imigrasi-di-era-yuldi-yusman-rekor-pnpb-dan-penguatan-penegakan-hukum
- Eastwood, S. C., Shmerko, V. P., Yanushkevich, S. N., Drahansky, M., & Gorodnichy, D. O. (2016). Biometric-enabled authentication machines: A survey of open-set real-world applications. *IEEE Transactions on Human-Machine Systems*, 46(2), 231–242.
- Eckhoff, T. (1975). The notion of basic norm(s) in jurisprudence. *Scandinavian Studies in Law*, 19, 121–152.
- FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).
- Gu, S., Feng, J., Lu, J., & Zhou, J. (2018). Efficient rectification of distorted fingerprints. *IEEE Transactions on Information Forensics and Security*, 13(1), 156–169.

- Jasserand, C. (2016). Legal nature of biometric data: From 'generic' personal data to sensitive data: Which changes does the new data protection framework introduce? *European Data Protection Law Review*, 2(3), 297–311.
- Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia. (2014). Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 8 Tahun 2014 tentang Paspor Biasa dan Surat Perjalanan Laksana Paspor (Berita Negara Republik Indonesia Tahun 2014 Nomor 649).
- Kementerian Imigrasi dan Pemasayarakatan Republik Indonesia. (2026). Peraturan Menteri Imigrasi dan Pemasayarakatan Nomor 11 Tahun 2026 tentang Paspor Biasa dan Surat Perjalanan Laksana Paspor (Berita Negara Republik Indonesia Tahun 2026 Nomor 521).
- Kumar, T., Bhushan, S., Sharma, P., & Garg, V. (2025). Examining the vulnerabilities of biometric systems: Privacy and security perspectives. In A. Selwal et al. (Eds.), *Leveraging computer vision to biometric applications*. CRC Press.
- Lubis, A. C. B., & Saraan, M. I. K. (2024). Efektivitas program Mobile Paspor dalam mendorong akuntabilitas pelayanan di Kantor Imigrasi Kelas I Khusus Kota Batam. *SAJJANA: Public Administration Review*, 2(1), 26–30.
- Lutfianingtyas, R. (2025). Data biometrik, taruhan tinggi: Memahami kewajiban hukum dan risiko dalam pengolahan data biometrik. *Indonesian Law Digest*, Edisi 956.
- Lutfianingtyas, R. (2026). Kementerian Imigrasi rombak layanan paspor: Masa berlaku lima tahun diberlakukan bagi pekerja migran dan penerima beasiswa. *Indonesian Legal Brief*, Edisi 5568.
- Machmudi, E. A. A. P. (2025). Navigating the institutional vacuum of personal data protection and public trust in Indonesia. *International Journal of Law Dynamics Review*, 3(2), 113–123.
- Mahkamah Konstitusi Republik Indonesia. (2025). Putusan Mahkamah Konstitusi Nomor 151/PUU-XXII/2024 perihal Pengujian Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Mills, J. L., & Harclerode, K. (2017). Privacy, mass intrusion, and the modern data breach. *Florida Law Review*, 69(3), 771–830.
- Neto, N. N., Madnick, S., de Paula, A. M. G., & Borges, N. M. (2020). A case study of the Capital One data breach (Revised) (Working Paper CISL# 2020-16). Sloan School of Management, Massachusetts Institute of Technology.
- Razmetaeva, Y. (2017, 27–28 April). Hybrid war, information technologies and the legal vacuum in the digital world [Makalah]. 5th International Conference of PhD Students and Young Researchers: How Deep Is Your Law? Brexit. Technologies. Modern Conflicts, Vilnius, Lithuania.
- Republik Indonesia. (1945). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Republik Indonesia. (2011a). Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234).
- Republik Indonesia. (2011b). Undang-Undang Nomor 6 Tahun 2011 tentang Keimigrasian (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 52, Tambahan Lembaran Negara Republik Indonesia Nomor 5216).
- Republik Indonesia. (2013). Peraturan Pemerintah Nomor 31 Tahun 2013 tentang Peraturan Pelaksanaan Undang-Undang Nomor 6 Tahun 2011 tentang Keimigrasian (Lembaran Negara Republik Indonesia Tahun 2013 Nomor 68, Tambahan Lembaran Negara Republik Indonesia Nomor 5409).

- Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).
- Republik Indonesia. (2024). Peraturan Presiden Nomor 157 Tahun 2024 tentang Kementerian Imigrasi dan Pemasarakatan (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 353).
- Rodrigues, G. A. P., Serrano, A. L. M., Lemos, A. N. L. E., Canedo, E. D., de Mendonça, F. L. L., de Oliveira Albuquerque, R., Orozco, A. L. S., & Villalba, L. J. G. (2023). Understanding data breach from a global perspective: Incident visualization and data protection law review. *Data*, 9(27), 1–24.
- Salane, D. E. (2011). Are large-scale data breaches inevitable? In T. Saadawi & L. Jordan (Eds.), *Cyber infrastructure protection. Strategic Studies Institute, US Army War College*.
- Sefrianti, T. E., Himamunanto, A. R., & Setyawan, G. C. (2024). Model daktiloskopi digital berbasis metode komposisi PCA-Euclidean-HOG untuk menemukan rumus sidik jari. *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, 13(2), 1669–1677.
- Sinaga, E. M. C., & Putri, M. C. (2020). Formulasi legislasi perlindungan data pribadi dalam revolusi industri 4.0. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 9(2), 237–256.
- Surya, I., & Wahab, A. (2023). Harmonisasi peraturan perundang-undangan dalam mewujudkan pemerintahan yang baik. *Jurnal Kompilasi Hukum*, 8(2), 108–117.
- Yang, W., Wang, S., Cui, H., Tang, Z., & Li, Y. (2023). A review of homomorphic encryption for privacy-preserving biometrics. *Sensors*, 23(7), 1–23.
- Yeovandi, F., Sabariman, S., & Prasetyo, S. E. (2025). Evaluasi keamanan sistem autentikasi biometrik pada smartphone dan rekomendasi implementasi optimal. *JTIM: Jurnal Teknologi Informasi dan Multimedia*, 7(1), 133–148.
- Yordanov, A. (2017). Nature and ideal steps of the data protection impact assessment under the General Data Protection Regulation. *European Data Protection Law Review*, 3(4), 486–495.