Journal Evidence of Law
Vol 5 No 2 2026, 771-781
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

Pengawasan dan Pertanggungjawaban Hukum atas Pemrosesan Data Pribadi Pelamar Kerja dalam Sistem Rekrutmen Elektronik

[1]Riza Faizah Achmad, [2]Hwian Christianto
[1,2]Universitas Surabaya, Surabaya, Indonesia
e-mail: [1]rizafaizah813@gmail.com, [2]hw_christianto@staff.ubaya.ac.id

Article History
Submission : 05-06-2026
Received : 09-07-2026
Revised : 31-07-2026
Accepted : 02-08-2026

Abstract

This study analyzes the legal status of the relevant actors, supervisory mechanisms, and forms of legal accountability in the reported public accessibility of applicants' documents during the 2026 recruitment of individual service providers by the Directorate General of Digital Infrastructure, Ministry of Communication and Digital Affairs. It employs normative legal research with statutory, conceptual, and case approaches. Legal materials are examined through grammatical, systematic, and teleological interpretation, while the recruitment notice and media reports are treated as supporting materials that do not substitute for an official investigation. The study finds that the recruiting unit may function as both a Personal Data Controller and a public-sector Electronic System Provider. A cloud-storage provider may qualify as a Personal Data Processor only where the factual and contractual relationship demonstrates processing on behalf of the Controller. If established, an open-access configuration indicates potential non-compliance with duties of security, confidentiality, supervision, prevention of unauthorized access, and accountability. Legal consequences may include corrective measures and breach notification, administrative sanctions, civil compensation, public-service disciplinary responsibility, and criminal liability where intent and unlawful conduct are proven. The analysis confirms that a lawful recruitment purpose does not displace the obligation to implement privacy by design and privacy by default.

Keywords: *Electronic system, Job applicant data, Legal accountability, Personal data controller, Right to privacy*

Abstrak

Penelitian ini menganalisis kedudukan hukum para pihak, mekanisme pengawasan, dan bentuk pertanggungjawaban hukum dalam dugaan keterbukaan akses dokumen pelamar pada rekrutmen Pengadaan Jasa Lainnya Perorangan Direktorat Jenderal Infrastruktur Digital Kementerian Komunikasi dan Digital tahun 2026. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Bahan hukum dianalisis melalui interpretasi gramatikal, sistematis, dan teleologis, sedangkan pemberitaan dan dokumen pengumuman rekrutmen diperlakukan sebagai bahan pendukung yang tidak menggantikan hasil pemeriksaan resmi. Hasil penelitian menunjukkan bahwa unit penyelenggara rekrutmen secara fungsional dapat berkedudukan sebagai Pengendali Data Pribadi sekaligus Penyelenggara Sistem Elektronik lingkup publik, sedangkan penyedia layanan penyimpanan hanya dapat dikualifikasikan sebagai Prosesor Data Pribadi berdasarkan hubungan faktual dan kontraktualnya. Konfigurasi akses terbuka, apabila terbukti, mengindikasikan ketidaksesuaian dengan kewajiban keamanan, kerahasiaan, pengawasan, pencegahan akses tidak sah, dan akuntabilitas. Pertanggungjawaban dapat mencakup tindakan korektif dan notifikasi insiden, sanksi administratif, gugatan ganti rugi, disiplin aparatur, serta pidana apabila unsur kesengajaan

This is an open access article under the CC BY-SA license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara

Journal Evidence of Law
Vol 5 No 2 2026, 771-781
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

dan perbuatan melawan hukum terpenuhi. Temuan ini menegaskan bahwa legitimasi pemrosesan untuk rekrutmen tidak menghapus kewajiban menerapkan privacy by design dan privacy by default.
Kata Kunci: Data pelamar kerja, Hak privasi, Pengendali data pribadi, Pertanggungjawaban hukum, Sistem elektronik.

Pendahuluan

Pelindungan data pribadi merupakan bagian dari pelindungan diri pribadi dan hak atas rasa aman yang dijamin oleh Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) kemudian menempatkan pelindungan data sebagai rangkaian kewajiban yang melekat pada setiap pihak yang menentukan tujuan, mengendalikan, atau melaksanakan pemrosesan data pribadi. Dengan demikian, keamanan data tidak hanya menjadi persoalan teknis, tetapi juga menjadi kewajiban hukum yang berkaitan dengan martabat, otonomi, dan kendali individu atas informasi tentang dirinya.

Digitalisasi rekrutmen mempercepat penerimaan dan pemeriksaan dokumen, tetapi sekaligus meningkatkan risiko keterbukaan data yang tidak diperlukan. Dokumen pelamar pada umumnya memuat nama, alamat, nomor telepon, riwayat pendidikan, pengalaman kerja, foto, tanda tangan, nomor identitas, dan dokumen pendukung. Surat keterangan sehat bahkan memuat informasi kesehatan yang dikategorikan sebagai data pribadi spesifik berdasarkan UU PDP. Karakter data tersebut menuntut pembatasan akses, keamanan penyimpanan, minimisasi pengumpulan, penentuan masa retensi, dan mekanisme penghapusan setelah tujuan rekrutmen berakhir.

Kasus yang menjadi objek kajian berkaitan dengan Pengumuman Nomor B-71/DJID.1/KP.03.01/01/2026 tentang Penerimaan Pengadaan Jasa Lainnya Perorangan di Lingkungan Direktorat Jenderal Infrastruktur Digital Tahun Anggaran 2026. Pengumuman tersebut meminta pelamar mengunggah surat lamaran dan dokumen pendukung melalui sebuah tautan yang diarahkan ke layanan penyimpanan daring. Berdasarkan pemberitaan Tempo.co pada 29 Januari 2026, dokumen yang telah diunggah sempat diduga dapat diakses secara terbuka oleh pengguna tautan. Tempo melaporkan bahwa pada 28 Januari 2026 pukul 19.00 WIB tautan tersebut telah dibatasi. Pemberitaan lanjutan pada 4 Februari 2026 menyebutkan bahwa Inspektorat Jenderal Komdigi melakukan pemeriksaan. Sampai batas bahan yang digunakan dalam penelitian ini, tidak ditemukan putusan atau hasil pemeriksaan resmi yang menetapkan secara final pihak, bentuk kesalahan, jumlah data yang terdampak, dan kerugian pelamar. Karena itu, penelitian menggunakan istilah dugaan keterbukaan akses atau indikasi ketidakpatuhan, bukan menyatakan pelanggaran yang telah terbukti.

Penelitian terdahulu telah membahas privacy by design, tata kelola pelindungan data, pelindungan data biometrik, hak privasi, serta penggunaan informasi pelamar dalam hubungan kerja (Caturjayanti, 2020; Drake et al., 2016; Hassan, 2012; Purtova, 2018; Sembiring et al., 2024; Sulistianingsih et al., 2023). Namun, kajian yang secara khusus memetakan kedudukan badan publik sebagai Pengendali Data Pribadi sekaligus Penyelenggara Sistem Elektronik, hubungan hukumnya dengan penyedia layanan penyimpanan, mekanisme pengawasan internal dan eksternal, kewajiban notifikasi, serta bentuk pertanggungjawaban berlapis dalam rekrutmen elektronik Indonesia masih terbatas.

Kebaruan penelitian ini terletak pada konstruksi pemisahan rezim kewajiban Pengendali Data Pribadi, Prosesor Data Pribadi, dan Penyelenggara Sistem Elektronik dalam satu proses rekrutmen instansi publik. Artikel juga menghubungkan pengawasan

This is an open access article under the CC BY-SA license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara

Journal Evidence of Law
Vol 5 No 2 2026, 771-781
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

internal, fungsi pejabat pelindungan data, notifikasi kegagalan pelindungan data, hak pelamar, dan pertanggungjawaban administratif, perdata, pidana, jabatan, serta institusional. Analisis tersebut penting karena penggunaan platform pihak ketiga tidak memindahkan secara otomatis tanggung jawab Pengendali Data Pribadi.

Berdasarkan uraian tersebut, penelitian ini mengajukan tiga masalah. Pertama, bagaimana kedudukan hukum para pihak yang memproses data pelamar dalam rekrutmen elektronik Komdigi? Kedua, bagaimana mekanisme pengawasan dan kewajiban pelindungan data pribadi pelamar berdasarkan UU PDP dan regulasi sistem elektronik? Ketiga, bagaimana bentuk pertanggungjawaban hukum apabila data pelamar dapat diakses oleh pihak yang tidak berwenang? Penelitian bertujuan menjawab ketiga masalah tersebut melalui analisis normatif terhadap kewajiban, potensi ketidakpatuhan, dan konsekuensi hukumnya.

Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif yang menempatkan norma, asas, dan konstruksi tanggung jawab hukum sebagai objek analisis. Pendekatan yang digunakan terdiri atas pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus. Pendekatan perundang-undangan digunakan untuk menelaah UUD NRI Tahun 1945, UU PDP, Undang-Undang Informasi dan Transaksi Elektronik sebagaimana terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 sepanjang masih relevan dan tidak bertentangan dengan UU PDP.

Pendekatan konseptual digunakan untuk mengkaji hak privasi, privacy by design, privacy by default, akuntabilitas, minimisasi data, retensi, serta pembedaan Pengendali Data Pribadi, Prosesor Data Pribadi, dan Penyelenggara Sistem Elektronik. Pendekatan kasus tidak digunakan dalam arti menelaah putusan pengadilan, melainkan untuk menerapkan norma pada peristiwa yang terdokumentasi dalam Pengumuman Nomor B-71/DJID.1/KP.03.01/01/2026, pemberitaan media, dan informasi publik terkait rekrutmen.

Bahan hukum primer terdiri atas peraturan perundang-undangan dan dokumen pengumuman rekrutmen. Bahan hukum sekunder meliputi artikel jurnal, buku, laporan, dan pemberitaan yang relevan. Pemberitaan diperlakukan sebagai bahan nonhukum pendukung untuk membangun kronologi awal, bukan sebagai bukti final terjadinya pelanggaran. Keabsahan peristiwa diverifikasi secara terbatas melalui kesesuaian antara nomor pengumuman resmi, persyaratan dokumen, tautan pendaftaran, dan lebih dari satu laporan publik. Informasi yang tidak tersedia, seperti durasi pasti keterbukaan akses, jumlah dokumen terdampak, konfigurasi teknis, kontrak dengan penyedia layanan, notifikasi kepada pelamar, dan hasil pemeriksaan Inspektorat Jenderal, dinyatakan sebagai keterbatasan dan tidak diasumsikan.

Analisis dilakukan secara preskriptif melalui interpretasi gramatikal untuk memahami istilah dan kewajiban dalam UU PDP, interpretasi sistematis untuk menghubungkan UU PDP dengan rezim penyelenggaraan sistem elektronik, dan interpretasi teleologis untuk menilai tujuan pelindungan hak subjek data. Penelitian tidak mengukur efektivitas empiris pengawasan, tetapi menilai kecukupan norma, kesesuaian dugaan tindakan dengan kewajiban hukum, serta potensi pertanggungjawaban apabila fakta yang dilaporkan terbukti.

This is an open access article under the CC BY-SA license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara

Journal Evidence of Law
Vol 5 No 2 2026, 771-781
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

Hasil dan Pembahasan

Hak Privasi, Hak Pelamar, dan Prinsip Desain Privasi

Konsep modern mengenai privasi sering dikaitkan dengan Warren dan Brandeis (1890) yang menempatkan privasi sebagai hak untuk dibiarkan sendiri. Dalam konteks pemrosesan digital, privasi berkembang menjadi hak individu untuk mengetahui, mengendalikan, memperbaiki, membatasi, dan meminta penghapusan informasi tentang dirinya. UU PDP mengkonkretkan hak tersebut melalui hak memperoleh informasi mengenai identitas dan akuntabilitas pihak yang meminta data, hak melengkapi dan memperbaiki data, hak memperoleh akses dan salinan, hak mengakhiri pemrosesan dan menghapus data, hak menarik persetujuan, hak membatasi pemrosesan, serta hak menggugat dan menerima ganti rugi.

Data pelamar kerja harus diklasifikasikan berdasarkan sifat dan risikonya. KTP, curriculum vitae, ijazah, transkrip, dan surat pengalaman kerja memuat data pribadi umum dan data kombinasi yang dapat mengidentifikasi seseorang. Foto dan tanda tangan merupakan data pengenal dan dapat memperoleh karakter biometrik apabila diproses secara teknis untuk tujuan identifikasi unik. Surat keterangan sehat memuat data kesehatan yang merupakan data pribadi spesifik. Perbedaan klasifikasi tersebut memengaruhi tingkat pengamanan yang harus diterapkan dan dapat memicu kewajiban penilaian dampak apabila pemrosesan berisiko tinggi, berskala besar, atau menggunakan teknologi baru.

Privacy by design berarti pelindungan data ditempatkan sejak tahap perencanaan sistem, proses kerja, organisasi, kontrak, dan kebijakan, bukan ditambahkan setelah insiden. Prinsip ini mencakup penetapan tujuan, minimisasi data, pembatasan akses berdasarkan peran, enkripsi, pencatatan aktivitas, audit, retensi, penghapusan, penanganan insiden, dan evaluasi penyedia layanan. Privacy by default berarti konfigurasi bawaan memberikan tingkat pelindungan tertinggi: folder tidak terbuka untuk publik, dokumen tidak dapat dilihat oleh sesama pelamar, tautan tidak dapat dibagikan tanpa otorisasi, serta akses hanya diberikan kepada panitia yang membutuhkan.

ISO/IEC 27001:2022 dapat digunakan sebagai rujukan teknis tata kelola keamanan informasi, tetapi bukan dasar langsung untuk menyatakan pelanggaran atau menjatuhkan sanksi. Dasar kewajiban hukum tetap berasal dari UU PDP dan regulasi penyelenggaraan sistem elektronik. Dengan demikian, kegagalan kontrol akses harus diuji terutama terhadap kewajiban menjaga kerahasiaan, melakukan pengawasan, mencegah pemrosesan dan akses tidak sah, serta membuktikan akuntabilitas.

Tabel 1. Klasifikasi Data Pelamar dan Risiko Pelindungannya

Dokumen/Data	Klasifikasi	Risiko Utama	Kontrol yang Relevan
KTP dan identitas	Data umum dan data kombinasi pengenal	Pencurian identitas, penipuan, penyebaran alamat/NIK	Minimisasi, enkripsi, pembatasan akses, masking
CV, riwayat pendidikan dan pekerjaan	Data umum; dapat menjadi data pemrofilan	Diskriminasi, pemrofilan, penyalahgunaan kontak	Akses berbasis peran, tujuan terbatas, retensi
Foto dan tanda tangan	Data pengenal; berpotensi	Pemalsuan identitas dan autentikasi	Pembatasan unduh, watermark, keamanan

This is an open access article under the CC BY-SA license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara

Journal Evidence of Law
Vol 5 No 2 2026, 771-781
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

Dokumen/Data	Klasifikasi	Risiko Utama	Kontrol yang Relevan
	biometrik tergantung pemrosesan		penyimpanan
Surat keterangan sehat	Data kesehatan/data spesifik	Stigma, diskriminasi, kerugian privasi tinggi	Pengamanan lebih tinggi, kebutuhan dan proporsionalitas
Ijazah, transkrip, sertifikat	Data umum dan dokumen autentik	Pemalsuan, penggunaan tanpa hak	Kontrol akses, verifikasi tanpa penyebarluasan

Kronologi dan Batas Analisis Kasus Rekrutmen

Pengumuman resmi tertanggal 8 Januari 2026 membuka sembilan posisi PJLP dan mensyaratkan antara lain KTP, surat lamaran, curriculum vitae, surat keterangan sehat, ijazah, transkrip, dan surat pengalaman kerja. Pendaftaran dilakukan pada 12–15 Januari 2026 melalui tautan singkat yang mengarah ke layanan penyimpanan daring. Struktur pengumpulan tersebut menunjukkan bahwa unit rekrutmen menentukan tujuan pengumpulan, jenis dokumen, periode pendaftaran, dan cara penyerahan data.

Pemberitaan publik menyatakan bahwa tautan tersebut sempat mengarah pada folder yang dapat diakses oleh publik dan memungkinkan pengguna melihat dokumen pelamar. Pada saat media melakukan pemeriksaan pada 28 Januari 2026 pukul 19.00 WIB, akses dilaporkan telah dibatasi. Pemeriksaan internal oleh Inspektorat Jenderal kemudian diberitakan pada 4 Februari 2026. Fakta bahwa akses telah dibatasi dapat dikualifikasikan sebagai tindakan awal mitigasi, tetapi tidak membuktikan apakah kewajiban notifikasi, dokumentasi insiden, pemulihan, dan penilaian dampak telah dipenuhi.

Penelitian ini tidak menyamakan folder terbuka dengan putusan hukum tentang kebocoran data. Istilah kegagalan pelindungan data dalam Pasal 46 UU PDP mensyaratkan analisis atas terungkapnya data, waktu dan cara pengungkapan, serta penanganan dan pemulihan. Karena hasil pemeriksaan resmi dan konfigurasi teknis tidak tersedia, kesimpulan artikel bersifat kondisional: apabila dokumen dapat diakses atau diunduh oleh pihak yang tidak berwenang, keadaan tersebut berpotensi memenuhi unsur akses atau pengungkapan tidak sah dan memicu kewajiban korektif.

Kedudukan Hukum Para Pihak

UU PDP menentukan kedudukan para pihak berdasarkan fungsi, bukan semata-mata nama organisasi. Pengendali Data Pribadi adalah pihak yang menentukan tujuan dan melakukan kendali pemrosesan, sedangkan Prosesor Data Pribadi memproses data atas nama pengendali. PSE adalah pihak yang menyediakan, mengelola, atau mengoperasikan sistem elektronik. Satu entitas dapat memegang lebih dari satu kedudukan sekaligus.

Dalam rekrutmen yang dikaji, Direktorat Jenderal Infrastruktur Digital atau unit/panitia yang mendapat kewenangan menentukan tujuan rekrutmen, jenis dokumen, cara pengumpulan, dan penggunaan data secara fungsional merupakan bagian dari badan publik yang bertindak sebagai Pengendali Data Pribadi. Karena proses diselenggarakan melalui sistem elektronik untuk fungsi badan publik, Komdigi juga dapat berkedudukan

This is an open access article under the CC BY-SA license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara

Journal Evidence of Law
Vol 5 No 2 2026, 771-781
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

sebagai PSE lingkup publik. Panitia dan pegawai yang mengakses dokumen bertindak di bawah kendali Pengendali Data Pribadi dan harus diawasi berdasarkan Pasal 37 UU PDP.

Penyedia layanan penyimpanan daring tidak otomatis menjadi pihak yang memikul tujuan rekrutmen. Penyedia tersebut dapat berkedudukan sebagai Prosesor Data Pribadi apabila memproses data atas nama Komdigi berdasarkan hubungan layanan, instruksi, dan pembagian tanggung jawab. Namun, apabila hanya menyediakan infrastruktur standar tanpa diketahui kontrak dan pengaturan kendalinya, kedudukannya tidak dapat dipastikan hanya dari nama platform. Ketiadaan informasi kontraktual merupakan batas penting dalam menetapkan tanggung jawab prosesor.

Pihak ketiga yang mengakses, memperoleh, atau menggunakan data tanpa hak dapat dimintai tanggung jawab berdasarkan perbuatannya. Tanggung jawab pihak ketiga tidak menghapus kewajiban pengendali untuk menerapkan sistem yang aman dan mencegah akses tanpa hak.

Tabel 2. Pemetaan Kedudukan Hukum Para Pihak

Pihak	Kedudukan Potensial	Implikasi Kewajiban
Komdigi/unit rekrutmen	Pengendali Data Pribadi dan PSE lingkup publik	Menentukan dasar dan tujuan; menjamin keamanan; mengawasi pihak; membuktikan akuntabilitas
Panitia/pegawai	Personel di bawah kendali pengendali	Akses hanya sesuai tugas; menjaga kerahasiaan; tunduk pada pengawasan dan disiplin
Penyedia cloud	PSE dan mungkin Prosesor Data Pribadi	Bergantung kontrak dan instruksi; keamanan dan pemrosesan atas nama pengendali
Pelamar	Subjek Data Pribadi	Memiliki hak informasi, akses, koreksi, penghapusan/pembatasan, dan ganti rugi
Pengakses tanpa hak	Pihak ketiga	Dapat bertanggung jawab jika memperoleh, mengungkapkan, atau menggunakan data secara melawan hukum

Dasar Pemrosesan, Minimisasi, dan Retensi

Pemrosesan data dalam rekrutmen harus memiliki dasar sebagaimana Pasal 20 UU PDP. Dasar yang paling relevan dapat berupa tindakan untuk memenuhi permintaan subjek data sebelum memasuki perjanjian, pelaksanaan tugas pelayanan publik atau kewenangan badan publik, dan dalam kondisi tertentu persetujuan eksplisit. Persetujuan bukan satu-satunya dasar dan tidak boleh digunakan untuk membenarkan pengumpulan yang berlebihan. Apapun dasar yang dipilih, pengendali tetap wajib menyampaikan legalitas, tujuan, jenis dan relevansi data, masa retensi, jangka waktu pemrosesan, serta hak subjek data.

Prinsip minimisasi menuntut panitia membedakan dokumen yang dibutuhkan pada tahap pendaftaran dan dokumen yang baru diperlukan setelah peserta dinyatakan lulus. Contohnya, verifikasi dokumen asli dapat dilakukan pada tahap akhir tanpa membuka seluruh salinan kepada banyak personel pada tahap awal. Surat keterangan sehat yang memuat data spesifik harus dikumpulkan hanya ketika benar-benar diperlukan dan diberikan tingkat perlindungan lebih tinggi.

This is an open access article under the CC BY-SA license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara

Journal Evidence of Law
Vol 5 No 2 2026, 771-781
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

Masa retensi harus dikaitkan dengan tujuan seleksi, kebutuhan pertanggungjawaban pengadaan, pengelolaan arsip, dan kemungkinan sengketa. Data pelamar yang tidak lolos tidak boleh disimpan tanpa batas. Setelah tujuan dan masa retensi berakhir, data harus dihapus, dimusnahkan, atau dianonimkan sesuai Pasal 42–45 UU PDP dan jadwal retensi arsip yang berlaku. Pengendali juga perlu menetapkan siapa yang dapat mengakses, kapan akses dicabut, dan bagaimana pemusnahan dibuktikan.

Praktik rekrutmen Komdigi pada seleksi lain yang dipublikasikan kemudian pada 2026 telah memuat keterangan pemrosesan data, tujuan, kategori data, pembatasan akses, retensi, serta kontak panitia. Praktik tersebut dapat menjadi model tata kelola, tetapi tidak dapat dianggap sebagai bukti penyelesaian atau pengakuan kesalahan pada kasus Januari 2026.

Mekanisme Pengawasan

Pengawasan pertama bersifat internal dan melekat pada Pengendali Data Pribadi. Pasal 37 UU PDP mewajibkan pengendali mengawasi setiap pihak yang terlibat dalam pemrosesan di bawah kendalinya. Pengawasan tersebut harus diwujudkan melalui matriks kewenangan, autentikasi pengguna, prinsip least privilege, pencatatan akses, peninjauan konfigurasi, audit berkala, pembatasan unduh, dan pencabutan hak akses ketika tugas selesai. PP Nomor 71 Tahun 2019 juga mengharuskan PSE memiliki tata kelola, prosedur operasional, serta mekanisme audit berkala.

Untuk badan publik, Pasal 53 dan Pasal 54 UU PDP mengharuskan penunjukan pejabat atau petugas yang melaksanakan fungsi pelindungan data pada pemrosesan untuk pelayanan publik. Fungsi ini mencakup pemberian saran, pemantauan kepatuhan, pemberian saran penilaian dampak, dan koordinasi isu pemrosesan. Pejabat tersebut bukan sekadar petugas keamanan teknologi, tetapi fungsi kepatuhan yang harus memiliki independensi profesional dalam memberi peringatan dan rekomendasi.

Inspektorat Jenderal menjalankan pengawasan internal pemerintahan dan dapat memeriksa tata kelola, kepatuhan pegawai, serta tanggung jawab jabatan. Pengawasan ini berbeda dari fungsi lembaga pelindungan data yang diamanatkan UU PDP untuk melaksanakan kebijakan, pengawasan, penegakan administratif, dan fasilitasi penyelesaian sengketa. Pengawasan internal tidak boleh menggantikan mekanisme eksternal, khususnya ketika instansi yang diperiksa juga memiliki fungsi regulasi pada sektor digital.

Pengawasan setelah insiden meliputi isolasi akses, pencatatan waktu dan ruang lingkup insiden, penilaian data terdampak, pengamanan bukti, evaluasi penyedia layanan, pemberitahuan kepada subjek data dan lembaga paling lambat 3 x 24 jam apabila terjadi kegagalan pelindungan data, serta dokumentasi upaya pemulihan. Pasal 46 UU PDP menetapkan bahwa pemberitahuan setidaknya memuat data yang terungkap, waktu dan cara keterungkapannya, serta upaya penanganan dan pemulihan.

Pertanggungjawaban Hukum

Pertanggungjawaban Pengendali Data Pribadi dibangun berdasarkan kewajiban hukum, tindakan atau kelalaian, keterbukaan atau akses tidak sah, kesalahan, kerugian atau risiko kerugian, dan hubungan kausal. Dalam kasus yang dikaji, kewajiban hukum dapat ditelusuri pada Pasal 35–39 dan Pasal 47 UU PDP. Namun, penetapan kesalahan memerlukan pemeriksaan mengenai konfigurasi akses, pihak yang mengubah pengaturan, waktu keterbukaan, jumlah dokumen, tindakan pengamanan, dan apakah akses benar-benar dilakukan oleh pihak yang tidak berwenang.

This is an open access article under the CC BY-SA license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara

Journal Evidence of Law
Vol 5 No 2 2026, 771-781
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

Pertanggungjawaban administratif dapat berupa peringatan tertulis, penghentian sementara pemrosesan, penghapusan atau pemusnahan data, dan denda administratif berdasarkan Pasal 57 UU PDP. Penerapan denda terhadap badan publik harus memperhatikan desain pengenaan sanksi dan variabel pelanggaran; tidak tepat menyamakan penerimaan badan publik secara sederhana dengan pendapatan perusahaan komersial. Di samping sanksi, tindakan korektif harus mencakup pembatasan akses, audit, penggantian media pengumpulan, pemulihan, dan notifikasi.

Pertanggungjawaban perdata timbul apabila subjek data dapat menunjukkan pelanggaran pemrosesan dan kerugian. Pasal 12 UU PDP memberikan hak untuk menggugat dan menerima ganti rugi. Kerugian dapat berupa biaya pemulihan identitas, penipuan, penggunaan dokumen tanpa hak, kehilangan kesempatan, serta kerugian imaterial karena hilangnya kendali dan rasa aman. Kausalitas harus dinilai secara konkret dan tidak dapat diasumsikan hanya karena data pernah berada dalam folder yang diduga terbuka.

Pertanggungjawaban pidana tidak otomatis timbul dari setiap kesalahan konfigurasi. Ketentuan pidana UU PDP terutama mensyaratkan perbuatan memperoleh, mengungkapkan, atau menggunakan data pribadi milik orang lain secara sengaja dan melawan hukum. Karena itu, kelalaian pengamanan harus dibedakan dari tindakan sengaja pihak yang mengambil atau menyebarluaskan data. Apabila pegawai dengan sengaja membuka, menyalin, atau menyebarkan data tanpa hak, pertanggungjawaban pidana dapat dipertimbangkan sesuai unsur yang terbukti.

Pertanggungjawaban disiplin atau jabatan dapat dikenakan kepada aparatur atau panitia yang tidak mematuhi prosedur, melampaui kewenangan akses, atau mengabaikan standar pengamanan. Pertanggungjawaban institusional tetap melekat pada badan publik dalam bentuk perbaikan tata kelola, audit independen, penunjukan fungsi pelindungan data, pelatihan, evaluasi vendor, dan pelaporan kepada publik. Tanggung jawab institusi tidak boleh direduksi menjadi kesalahan individual apabila desain sistem dan prosedurnya memang tidak memadai.

Tabel 3. Bentuk Pertanggungjawaban dan Prasyaratnya

Bentuk	Dasar/Prasyarat	Konsekuensi Potensial
Korektif dan notifikasi	Terjadi kegagalan pelindungan data	Pembatasan akses, investigasi, pemulihan, pemberitahuan 3 x 24 jam
Administratif	Ketidakpatuhan kewajiban pengendali/prosesor	Peringatan, penghentian pemrosesan, penghapusan/pemusnahan, denda
Perdata	Pelanggaran, kerugian, dan hubungan kausal	Gugatan dan ganti rugi material atau imaterial
Pidana	Kesengajaan dan perbuatan melawan hukum	Pidana bagi pihak yang memperoleh, mengungkapkan, atau menggunakan data tanpa hak
Disiplin/jabatan	Pelanggaran prosedur atau kewajiban aparatur	Pemeriksaan dan sanksi kepegawaian
Institusional	Kelemahan desain, tata kelola, atau pengawasan	Audit, revisi SOP, pelatihan, DPO, evaluasi vendor, pelaporan

This is an open access article under the CC BY-SA license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara

Journal Evidence of Law
Vol 5 No 2 2026, 771-781
E-ISSN: 2828-5031 | P-ISSN: 2830-3350
Publisher: CV. Era Digital Nusantara
Website: https://jurnal.erapublikasi.id/index.php/JEL

Model Pencegahan pada Rekrutmen Elektronik

Model pencegahan harus menggabungkan aspek hukum, organisasi, dan teknis. Pada tahap perencanaan, instansi menetapkan dasar dan tujuan pemrosesan, memetakan data yang benar-benar diperlukan, melakukan penilaian risiko, menentukan masa retensi, serta memilih platform yang menyediakan autentikasi, pembatasan akses, pencatatan aktivitas, dan kemampuan penghapusan. Kontrak dengan penyedia layanan harus mengatur instruksi pemrosesan, lokasi penyimpanan, subprosesor, keamanan, bantuan penanganan insiden, audit, pengembalian, dan pemusnahan data.

Pada tahap pengumpulan, portal harus menerapkan akun individual, unggahan privat, pemisahan folder, validasi jenis berkas, enkripsi selama transmisi dan penyimpanan, serta pemberitahuan privasi yang mudah dipahami. Pemberitahuan harus memuat identitas pengendali, tujuan, dasar pemrosesan, kategori data, pihak yang memiliki akses, retensi, hak pelamar, kontak, dan mekanisme pengaduan. Tautan umum tanpa autentikasi tidak sesuai dengan prinsip pengaturan bawaan yang paling melindungi.

Pada tahap seleksi, akses diberikan berdasarkan peran dan kebutuhan. Panitia tidak boleh mengunduh atau menyalin dokumen ke perangkat pribadi tanpa pengamanan. Aktivitas akses harus dicatat dan ditinjau. Setelah seleksi, akses panitia ditutup, dokumen peserta yang tidak diterima dikelola sesuai retensi, dan data yang tidak diperlukan dihapus atau dianonimkan.

Pada tahap respons insiden, instansi harus memiliki prosedur deteksi, eskalasi, isolasi, penilaian dampak, komunikasi, notifikasi, pemulihan, dan pembelajaran. Pelatihan panitia harus dilakukan sebelum pendaftaran dibuka. Audit konfigurasi wajib menjadi bagian dari daftar periksa pra-peluncuran, bukan hanya dilakukan setelah muncul keluhan.

Kesimpulan

Pertama, unit Komdigi yang menentukan tujuan, jenis dokumen, sarana pengumpulan, dan penggunaan data pelamar secara fungsional berkedudukan sebagai Pengendali Data Pribadi dan dapat sekaligus menjadi PSE lingkup publik. Panitia bertindak di bawah kendali pengendali, sedangkan penyedia layanan penyimpanan hanya dapat dikualifikasikan sebagai Prosesor Data Pribadi apabila hubungan faktual dan kontraktual menunjukkan pemrosesan atas nama pengendali. Pembedaan tersebut penting karena kewajiban berdasarkan UU PDP dan kewajiban berdasarkan rezim sistem elektronik tidak dapat dicampuradukkan.

Kedua, pengawasan meliputi pengawasan internal Pengendali Data Pribadi, fungsi pejabat pelindungan data, audit sistem elektronik, pengawasan Inspektorat Jenderal, dan pengawasan eksternal berdasarkan kelembagaan UU PDP. Konfigurasi akses terbuka, apabila terbukti, berpotensi tidak sesuai dengan kewajiban keamanan, kerahasiaan, pengawasan, pencegahan akses tidak sah, dan akuntabilitas. Kejadian tersebut juga dapat memicu kewajiban notifikasi tertulis paling lambat 3 x 24 jam dan tindakan pemulihan.

Ketiga, pertanggungjawaban tidak terbatas pada sanksi administratif. Konsekuensinya dapat berupa tindakan korektif, penghapusan atau pembatasan pemrosesan, gugatan ganti rugi, disiplin aparatur, tanggung jawab institusional, dan pidana apabila unsur kesengajaan serta perbuatan melawan hukum terpenuhi. Karena penelitian hanya menggunakan dokumen publik dan pemberitaan, artikel tidak menyimpulkan pelanggaran final, melainkan menunjukkan konstruksi kewajiban dan konsekuensi yang berlaku apabila dugaan fakta dapat dibuktikan.

Penelitian tidak memperoleh hasil pemeriksaan resmi Inspektorat Jenderal, data jumlah pelamar terdampak, log akses, durasi pasti keterbukaan folder, konfigurasi teknis,

This is an open access article under the CC BY-SA license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara

kontrak penyedia layanan, atau bukti notifikasi kepada pelamar. Oleh karena itu, analisis tidak menetapkan pihak yang bersalah dan tidak mengukur efektivitas empiris pengawasan. Penelitian berikutnya perlu menggunakan pendekatan socio-legal melalui wawancara dengan pelamar, panitia, pengelola sistem, pejabat pelindungan data, Inspektorat Jenderal, dan penyedia layanan.

Daftar Pustaka

Caturjayanti, V. D. (2020). Konsep privacy by design sebagai pelindungan data pribadi pengguna aplikasi PeduliLindungi. Jurnal Hukum Lex Generalis, 1(9), 70–87. https://doi.org/10.56370/jhlg.v1i9.251

Cavoukian, A. (2011). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario.

Direktorat Jenderal Infrastruktur Digital. (2026). Pengumuman B-71/DJID.1/KP.03.01/01/2026 tentang penerimaan PJLP tahun anggaran 2026; Kementerian Komunikasi dan Digital. (2026). Portal seleksi PJLP dan ketentuan pemrosesan data pribadi.

Drake, J. R., Hall, D., Becton, J. B., & Posey, C. (2016). Job applicants' information privacy protection responses: Using social media for candidate screening. AIS Transactions on Human-Computer Interaction, 8(4), 160–184.

Enerstvedt, O. M. (2017). Analysis of privacy and data protection principles. In Aviation security, privacy, data protection and other human rights (pp. 307–394). Springer. https://doi.org/10.1007/978-3-319-58139-2_7

Hassan, K. H. (2012). Personal data protection in employment: New legal challenges for Malaysia. Computer Law & Security Review, 28(6), 696–703. https://doi.org/10.1016/j.clsr.2012.09.005

International Organization for Standardization. (2022). ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—Information security management systems—Requirements.

Kusnadi, S. A. (2021). Perlindungan hukum data pribadi sebagai hak privasi. AL WASATH Jurnal Ilmu Hukum, 2(1), 9–16. https://doi.org/10.47776/alwasath.v2i1.127

Kusnadi, S. A., & Putri, D. W. S. (2025). Perlindungan hak privasi dalam penyalahgunaan teknologi deepfake di Indonesia. Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional, 14(2).

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Purtova, N. (2018). The law of everything: Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, 10(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Rima, K., Suari, A., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Pelindungan data pribadi di Indonesia. Jurnal Analisis Hukum, 6(1), 132–146. https://doi.org/10.38043/jah.v6i1.4484

Romadhona, I. A., & Kusnadi, S. A. (2023). Legal responsibility of Hootsuite in the crime of misuse of personal data. Budapest International Research and Critics Institute Journal, 6(1), 315–321. https://doi.org/10.33258/birci.v6i1.7459

Salfutra, R. D. (2018). Hak asasi manusia dalam perspektif filsafat hukum. Progresif: Jurnal Hukum, 12(2), 2146–2158. https://doi.org/10.33019/progresif.v12i2.977

This is an open access article under the CC BY-SA license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara

Sembiring, P. E., Ramli, A. M., & Rafianti, L. (2024). Implementasi desain privasi sebagai pelindungan privasi atas data biometrik. Veritas et Justitia, 10(1), 127–152. https://doi.org/10.25123/vej.v10i1.7622

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–560.

Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata kelola pelindungan data pribadi di era metaverse: Telaah yuridis Undang-Undang Pelindungan Data Pribadi. Masalah-Masalah Hukum, 52(1), 97–106. https://doi.org/10.14710/mmh.52.1.2023.97-106

Tempo.co. (2026a, January 29). Data pribadi pelamar Komdigi diduga bocor, publik bisa akses.

Tempo.co. (2026b, February 4). Irjen usut loker Komdigi langgar perlindungan data pribadi.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220. https://doi.org/10.2307/1321160

This is an open access article under the CC BY-SA license.
Copyright© 2026 by Author. Published by CV. Era Digital Nusantara