Jurnal Infosecure Vol.6 No.1, April 2025
p-ISSN: 2087-1023
MTI-UNLA

Tata Kelola Keamanan Data Pribadi Berdasarkan Indeks Kami Untuk Mendukung Kepatuhan Terhadap Uu No. 27 Tahun 2022 Pada Lembaga Sertifikasi Profesi

Tsaltsa Nurussalamah[1], Hendra Sandhi Firmansyah[2], Mokhamad Hendayun[3]

Magister Teknik Informatika, Universitas Langlangbuana[1,2,3]

[1]nurussalamahtsaltsa@gmail.com

[2]hendra.sf@gmail.com

[3]mhendayun@gmail.com

Abstrak— Pesatnya perkembangan teknologi informasi menuntut Lembaga Sertifikasi Profesi (LSP) untuk menerapkan tata kelola keamanan data pribadi yang sesuai dengan regulasi, khususnya UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Penelitian ini bertujuan mengevaluasi kesiapan LSP dalam pelindungan data pribadi menggunakan Indeks KAMI versi 5.0 dan memetakan indikatornya terhadap pasal-pasal UU PDP. Penelitian dilakukan dengan pendekatan deskriptif kualitatif melalui studi kasus pada satu LSP resmi di bawah BNSP. Hasil menunjukkan bahwa tingkat kematangan tata kelola masih berada pada kategori "Cukup", dengan kelemahan pada dokumentasi kebijakan, penunjukan DPO, dan prosedur pengelolaan risiko. Sebagai rekomendasi, disusun sembilan SOP yang dapat diterapkan LSP untuk meningkatkan kepatuhan. Penelitian ini berkontribusi dalam pengembangan tata kelola keamanan data pribadi yang terukur, terstruktur, dan aplikatif sesuai ketentuan hukum nasional.

Kata kunci— Tata Kelola, Keamanan Data Pribadi, Indeks KAMI, UU PDP, LSP

I. Pendahuluan

Perkembangan teknologi menuntut organisasi untuk terus beradaptasi dan mengoptimalkan pemanfaatan teknologi informasi. Hal ini mendorong peningkatan jumlah informasi yang dikelola, sehingga keamanan informasi menjadi elemen penting yang mencakup perlindungan hardware, pusat data, dan jaringan. Keamanan ini harus mencakup aspek kerahasiaan, integritas, dan ketersediaan data [Chaesya, 2021].

Tata kelola yang baik (good governance) mencakup pengambilan keputusan dan pengelolaan sumber daya secara transparan, akuntabel, adil, dan berkelanjutan [Hidayah A, 2023; Saputra C Deannova, dkk, 2024]. Dalam konteks ini, Lembaga Sertifikasi Profesi (LSP) bertanggung jawab mengelola data pribadi peserta sertifikasi, seperti NIK, riwayat pendidikan, dan dokumen pendukung lainnya, yang wajib dilindungi dari penyalahgunaan demi menjaga privasi dan kepercayaan publik [Kemenkeu; Pilo R, 2023].

Tata kelola LSP mencakup sistem manajemen yang terstruktur melalui visi, misi, struktur organisasi, kebijakan mutu, dan pemanfaatan teknologi informasi [BNSP]. Namun, masih terdapat tantangan seperti penyimpanan manual, kurangnya kebijakan pelindungan data, dan minimnya pelatihan keamanan informasi. Kondisi ini menunjukkan bahwa aspek pelindungan data belum sepenuhnya terintegrasi dalam sistem tata kelola LSP.

UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi dasar hukum pengelolaan data di Indonesia, meski masih bersifat normatif dan belum menyediakan instrumen evaluasi yang aplikatif [Christian David, 2022]. Sebagai solusi, BSSN merilis Indeks KAMI versi 5.0 sebagai alat ukur kesiapan dan kepatuhan terhadap prinsip keamanan informasi, mencakup enam domain utama, termasuk pelindungan data pribadi [Pratiwi A Hadiati & Wulandari Lily, 2021].

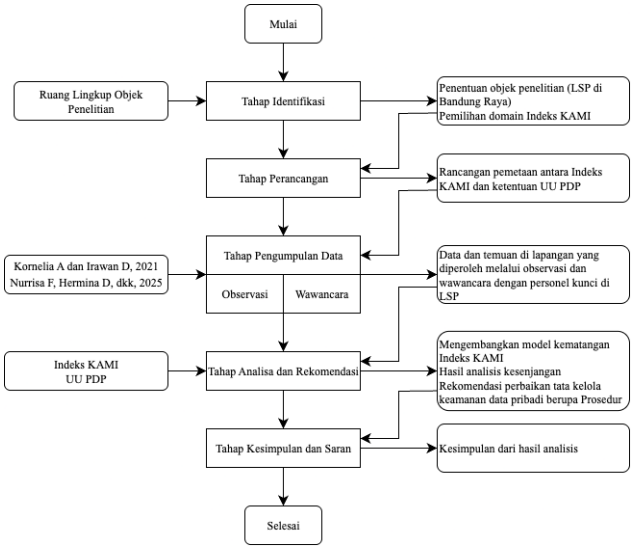
Konsep nilai kematangan dalam Indeks KAMI membantu LSP mengidentifikasi kelemahan, menentukan prioritas perbaikan, serta menyusun strategi peningkatan keamanan yang sesuai dengan UU PDP. Pendekatan ini mendukung akuntabilitas dan meningkatkan kepercayaan publik [BSSN].

Penelitian ini mengadopsi pendekatan evaluatif yang integratif, memadukan Indeks KAMI dengan UU PDP, serta fokus pada LSP sebagai objek kajian. Hasilnya adalah pengukuran tingkat kematangan tata kelola keamanan dan perancangan SOP siap pakai, yang memperkuat kontribusi praktis dibandingkan studi sebelumnya..

Berdasarkan uraian di atas, penelitian ini bertujuan untuk menganalisis kondisi tata kelola keamanan data pribadi pada LSP saat ini, mengidentifikasi metode pengukuran tingkat kematangan tata kelola , menentukan kondisi ideal tata kelola berdasarkan Indeks KAMI , melakukan pemetaan Indeks KAMI dengan UU PDP , serta menyusun prosedur tata kelola keamanan data pribadi yang dapat diterapkan oleh LSP. Penelitian ini menggunakan metode terapan dengan pendekatan kualitatif deskriptif , melibatkan observasi dan wawancara sebagai metode pengumpulan data.

II. Metode

Penelitian ini mengadopsi metode penelitian terapan dengan pendekatan kualitatif yang bersifat deskriptif. Penelitian terapan bertujuan untuk menghasilkan solusi aplikatif, yang dalam konteks ini adalah prosedur tata kelola keamanan data pribadi. Pendekatan kualitatif digunakan untuk menggambarkan kondisi faktual dan akurat mengenai tata kelola keamanan data pribadi pada Lembaga Sertifikasi Profesi (LSP).



Gambar II-1 Tahapan Penelitian

Tahapan penelitian yang dilakukan berdasarkan Indeks KAMI versi 5.0 dan ketentuan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi meliputi:

1. Tahap Identifikasi
   Menentukan ruang lingkup objek penelitian, yaitu LSP di wilayah Bandung Raya (Kota Bandung, Kota Cimahi, Kabupaten Bandung, dan Kabupaten Bandung Barat). Pemilihan domain Indeks KAMI difokuskan pada Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, dan Pelindungan Data Pribadi.
2. Tahap Perancangan
   Menyusun instrumen pengumpulan data berupa kuesioner berdasarkan indikator Indeks KAMI dan mengidentifikasi pasal-pasal UU PDP yang relevan (Pasal 1, 16, 17, 33, 35, 36, 42, dan 46). Instrumen ini dipetakan untuk melihat keterkaitan dan kesesuaian antar indikator.
3. Tahap Pengumpulan Data
   Dilakukan melalui observasi terhadap lingkungan kerja dan infrastruktur TI , serta wawancara langsung dengan tim IT, manajemen, dan pengelola data pribadi di enam LSP terpilih menggunakan *purposive sampling*. Jawaban dikonversi menjadi skor tingkat kematangan sesuai format Indeks KAMI.
4. Tahap Analisis dan Rekomendasi
   Menganalisis data dengan menghitung skor tingkat kematangan untuk setiap domain berdasarkan Indeks KAMI. Dilakukan *gap analysis* antara kondisi aktual LSP dengan standar UU PDP. Hasil analisis digunakan untuk menyusun rekomendasi perbaikan dan prosedur tata kelola keamanan data pribadi.
5. Tahap Kesimpulan dan Saran
   Merumuskan kesimpulan dari hasil analisis dan menyampaikan saran strategis untuk peningkatan keamanan data pribadi dan kepatuhan regulasi.

III. Hasil dan Pembahasan

A. *Objek Penelitian*

Penelitian ini mengkaji tata kelola keamanan data pribadi pada enam Lembaga Sertifikasi Profesi (LSP) di Bandung Raya (Kota Bandung, Cimahi, Kab. Bandung, dan Kab. Bandung Barat). Wilayah ini representatif karena memiliki sekitar 32 LSP dari jenis P1 dan P2. Pemilihan LSP dilakukan secara *purposive sampling* berdasarkan kriteria seperti jumlah asesi signifikan, skema sertifikasi terkait TI/data sensitif, keterbukaan evaluasi, ketersediaan dokumen, dan sistem manajemen data pribadi. Variasi jenis LSP (P1 dan P2) memungkinkan gambaran komprehensif terkait penerapan tata kelola keamanan data pribadi pada berbagai skala operasional. Identitas LSP disamarkan untuk menjaga kerahasiaan.

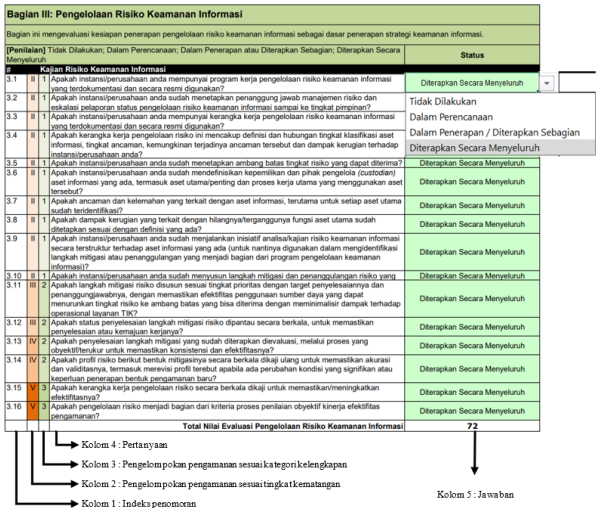
Tabel A-1 Daftar LSP Bandung Raya

Jenis LSP / Wilayah LSP	P1	P2
Kota Bandung	19	4
Kota Cimahi	5	1
Kab. Bandung	2	1

B. *Evaluasi Indeks KAMI*

Evaluasi Indeks KAMI ini berfungsi untuk menilai tingkat kesiapan dan kematangan tata kelola keamanan informasi di LSP. Penilaian dilakukan berdasarkan 54 pertanyaan Indeks KAMI versi 5.0, yang dibagi ke dalam tiga area utama: Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, dan Pelindungan Data Pribadi.

Tabel B-1 Evaluasi Indeks KAMI



Pertanyaan dan jawaban disajikan dalam format tabel, di mana setiap status penerapan dikonversi menjadi skor sesuai kategori pengamanan yang telah didefinisikan dalam Indeks KAMI. Perhitungan skor ini kemudian menentukan tingkat kematangan di setiap domain.

Tabel B-2 Skor Kategori Kelengkapan

Status Penerapan	Penetapan Skor		
	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Perencanaan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Penyesuaian bobot skor pada Indeks KAMI dilakukan untuk memastikan instrumen evaluasi mencerminkan secara representatif dan proporsional kondisi tata kelola keamanan data

pribadi. Penyesuaian ini didasarkan pada pertimbangan metodologis, relevansi dengan UU PDP, dan kebutuhan representasi hasil evaluasi yang akurat. Sebanyak 27 pertanyaan baru ditambahkan untuk menggali aspek-aspek krusial yang sebelumnya belum terakomodasi, sehingga memperluas cakupan dan meningkatkan keterbaruan skor evaluasi.

Tabel B-3 Skor Kategori Kelengkapan Keterbaharuan

Status Penerapan	Penetapan Skor Tata Kelola			Penetapan Skor Risiko			Penetapan Skor PDP		
	1	2	3	1	2	3	1	2	3
Tidak Dilakukan	0	0	0	0	0	0	0	0	0
Dalam Perencanaan	1	2	1	1	2	1	1	1	3
Dalam Perencanaan atau Diterapkan Sebagian	2	4	2	2	4	2	2	2	6
Diterapkan secara Menyeluruh	3	6	3	3	6	3	3	3	9

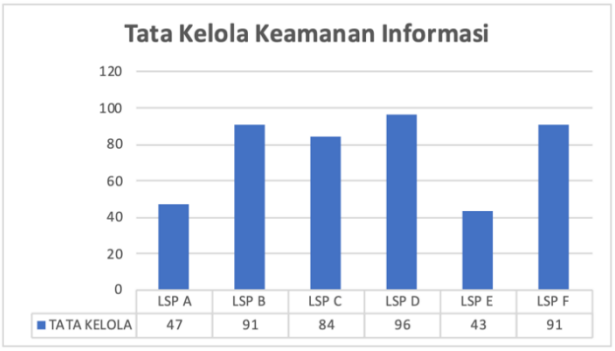
C. *Tata Kelola Keamanan Informasi*

Domain ini mengevaluasi kesiapan organisasi dalam membentuk struktur dan tanggung jawab pengelolaan keamanan informasi. Relevansi Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) terhadap domain tata kelola keamanan informasi dalam Indeks KAMI tercermin melalui tiga pasal kunci, yakni Pasal 1, Pasal 33, dan Pasal 35. Pasal 1 memberikan dasar konseptual mengenai definisi data pribadi, pengendali, pemrosesan, dan keamanan data, yang menjadi landasan dalam penyusunan kebijakan tata kelola keamanan informasi di tingkat organisasi. Sementara itu, Pasal 33 menegaskan tanggung jawab pengendali data untuk menjamin pemrosesan yang sesuai prinsip pelindungan data, termasuk kewajiban menunjuk petugas pelindungan data pribadi (DPO), menyusun dokumentasi, serta menjaga integritas dan kerahasiaan data. Pasal ini memperkuat pentingnya struktur organisasi, pembagian peran, dan kebijakan formal dalam tata kelola. Selanjutnya, Pasal 35 mewajibkan pengendali data untuk menerapkan sistem pengamanan yang memadai serta melakukan tindakan preventif terhadap risiko kebocoran atau akses ilegal, yang selaras dengan prinsip-prinsip tata kelola terkait mitigasi risiko dan pengambilan keputusan strategis dalam keamanan informasi. Ketiga pasal ini secara langsung mendukung indikator dalam domain tata kelola Indeks KAMI, khususnya dalam membangun sistem pengelolaan keamanan data pribadi yang berbasis hukum, terstruktur, dan akuntabel, dengan penambahan 11 pertanyaan baru yang selaras dengan UU PDP Pasal 1, 33, dan 35.

Tabel C-1 Irisan Tata Kelola dengan UU PDP

#			
UU PDP Pasal 1			
2.23	III	3	Apakah LSP memiliki kebijakan tertulis terkait pengelolaan dan perlindungan data pribadi?
2.24	III	3	Apakah kebijakan tersebut mengatur hak-hak subjek data pribadi sesuai dengan ketentuan UU PDP?
2.25	III	3	Apakah LSP memiliki prosedur terkait pengelolaan data pribadi yang melibatkan prosesor data?
UU PDP Pasal 33			
2.26	III	3	Apakah kebijakan pelindungan data pribadi mencakup ketentuan untuk melindungi keamanan data?
2.27	IV	3	Apakah terdapat pengawasan terhadap pihak ketiga (prosesor data) yang terlibat dalam pengelolaan data?
2.28	IV	3	Apakah LSP telah menerapkan mekanisme audit internal secara berkala terhadap pelaksanaan kebijakan pelindungan data pribadi dan memastikan hasil audit ditindaklanjuti untuk perbaikan berkelanjutan ?
UU PDP Pasal 35			
2.29	III	3	Apakah terdapat kebijakan yang mengatur pembatasan akses dan pengungkapan data pribadi?
2.30	IV	3	Apakah LSP memiliki mekanisme pemantauan untuk mendeteksi potensi gangguan pada data pribadi?
2.31	IV	3	Apakah LSP telah menerapkan langkah teknis operasional untuk melindungi data pribadi?
2.32	IV	3	Apakah terdapat dokumentasi terkait penerapan teknologi keamanan informasi pada data pribadi?
2.33	IV	3	Apakah tingkat keamanan data pribadi ditentukan berdasarkan risiko dan sifat data yang dilindungi?

Penilaian domain tata kelola keamanan informasi dilakukan untuk mengevaluasi sejauh mana suatu LSP telah membentuk struktur, kebijakan, dan mekanisme pengelolaan keamanan informasi secara formal dan terdokumentasi. Domain ini memiliki skor maksimum sebesar 126 poin.



Gambar III-1 Grafik Tata Kelola Keamanan Informasi

Dari analisis data dan visualisasi grafik tata Kelola keamanan informasi, dapat ditarik beberapa poin :

1. Variasi Tingkat Kesiapan
   a. Tinggi
      LSP D (skor 96) menunjukkan tingkat kesiapan tertinggi, dengan sebagian besar aspek tata kelola keamanan informasi telah "Diterapkan Secara Menyeluruh". LSP B dan LSP F (masing-masing skor 91) juga menunjukkan kesiapan yang sangat baik, dengan banyak area yang "Diterapkan Secara Menyeluruh" atau "Dalam Penerapan/Diterapkan Sebagian". Ketiga LSP ini memiliki kerangka kerja tata kelola yang matang dan komprehensif.
   b. Menengah
      LSP C (skor 84) berada pada tingkat menengah. Meskipun banyak aspek telah "Diterapkan Secara Menyeluruh", beberapa area masih "Dalam Perencanaan" atau "Dalam Penerapan/Diterapkan Sebagian". Ini menunjukkan kemajuan yang baik namun perlu perbaikan.
   c. Rendah
      LSP A (skor 47) dan LSP E (skor 43) memiliki tingkat kesiapan terendah. Banyak aspek tata kelola keamanan informasi di kedua LSP ini masih "Dalam Perencanaan" atau "Tidak Dilakukan", mengindikasikan perlunya upaya pengembangan yang signifikan untuk memperkuat kerangka kerja mereka.
2. Indikator Kinerja Tata Kelola dan Area untuk Peningkatan
   Total nilai evaluasi mencerminkan tingkat implementasi elemen-elemen kunci tata kelola keamanan informasi, seperti peran dan tanggung jawab, alokasi sumber daya, program sosialisasi, integrasi keamanan dalam proses kerja, pengelolaan data pribadi (termasuk kepatuhan UU PDP), serta mekanisme pengukuran kinerja. Nilai yang lebih tinggi menunjukkan adopsi dan penerapan yang lebih kuat terhadap praktik tata kelola yang direkomendasikan. Bagi LSP dengan nilai lebih rendah (A dan E), hasil ini menyoroti kebutuhan akan pengembangan kebijakan, penetapan prosedur, alokasi sumber daya memadai, peningkatan kompetensi personel, serta program berkelanjutan untuk memastikan kepatuhan dan efektivitas keamanan informasi.

D. *Pengelolaan Risiko Keamanan Informasi*

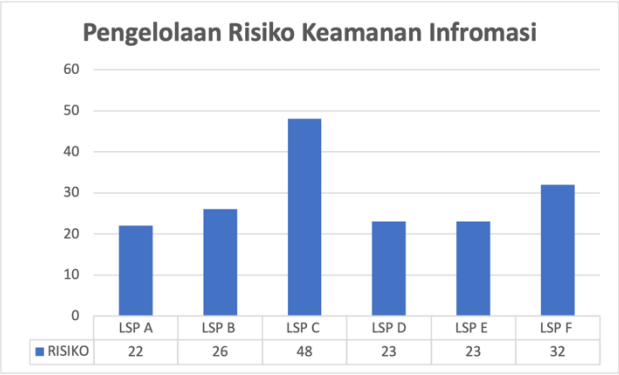
Pengelolaan risiko keamanan informasi, khususnya terkait data pribadi di Lembaga Sertifikasi Profesi (LSP), sangat relevan

dengan kewajiban yang diatur dalam Undang-Undang Perlindungan Data Pribadi (UU PDP). Pasal 36 UU PDP secara eksplisit mengamanatkan pengendali data untuk menjaga kerahasiaan data pribadi yang diproses, di mana LSP diwajibkan memiliki kebijakan tertulis formal dan prosedur operasional yang jelas untuk memastikan kerahasiaan data di setiap tahapan pemrosesan (misalnya, melalui otorisasi akses atau enkripsi). Sejalan dengan itu, Pasal 42 UU PDP mengatur mengenai masa retensi data pribadi, mewajibkan penghapusan atau pemusnahan data setelah masa retensi berakhir atau tujuan pemrosesan tercapai, kecuali ditentukan lain oleh peraturan perundang-undangan. Untuk memenuhi hal ini, LSP harus memiliki kebijakan yang jelas mengenai masa retensi data dan prosedur operasional untuk menghapus atau memusnahkan data secara aman, guna mengurangi risiko penyalahgunaan atau pelanggaran data di masa depan. Dengan demikian, kepatuhan terhadap kedua pasal ini merupakan aspek krusial dalam pengelolaan siklus hidup data dan mitigasi risiko keamanan informasi, dengan penambahan 4 pertanyaan baru yang selaras dengan UU PDP Pasal 36 dan Pasal 42

Tabel D-1 Irisan Pengelolaan Risiko dengan UU PDP

#			UU PDP Pasal 36	
3.17	III	3	Apakah LSP memiliki kebijakan tertulis terkait kerahasiaan data pribadi?	
3.18	IV	3	Apakah terdapat prosedur untuk menjaga kerahasiaan data pribadi selama pemrosesan data?	
#			UU PDP Pasal 42	
3.19	III	3	Apakah LSP memiliki kebijakan terkait masa retensi data pribadi?	
3.20	IV	3	Apakah terdapat prosedur untuk mengakhiri pemrosesan data pribadi sesuai masa retensi?	
			Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	

Penilaian domain pengelolaan risiko keamanan informasi dilakukan untuk mengevaluasi sejauh mana suatu LSP telah mengidentifikasi, menganalisis, mengevaluasi, mengobati, dan memantau risiko keamanan informasi secara sistematis dan terdokumentasi. Domain ini memiliki skor maksimum sebesar 72 poin.



Gambar III-2 Grafik Pengelolaan Risiko Keamanan Informasi

Dari analisis data dan visualisasi grafik pengelolaan risiko keamanan informasi, dapat ditarik beberapa poin :

1. Variasi Tingkat Kesiapan
   a. Tinggi
      LSP C memimpin dengan total nilai evaluasi 48. Ini menunjukkan bahwa LSP C telah mencapai status "Diterapkan Secara Menyeluruh" atau setidaknya "Dalam Penerapan/Diterapkan Sebagian" pada banyak aspek krusial pengelolaan risiko. LSP C memiliki pendekatan yang matang dan terstruktur dalam mengelola risiko keamanan informasi.
   b. Menengah
      LSP F berada di posisi kedua dengan nilai evaluasi 32. LSP F menunjukkan kemajuan dengan beberapa aspek kunci yang sudah "Diterapkan Secara Menyeluruh" seperti penetapan penanggung jawab dan penyusunan langkah mitigasi. Meskipun demikian, masih banyak area yang membutuhkan pengembangan lebih lanjut dari tahap "Dalam Perencanaan".
   c. Rendah
      LSP A (22), LSP B (26), LSP D (23), dan LSP E (23) memiliki nilai evaluasi yang relatif rendah dan sangat berdekatan. Mayoritas aspek dalam pengelolaan risiko keamanan informasi di LSP-LSP ini masih berada pada tahap "Dalam Perencanaan". Hal ini menunjukkan bahwa LSP-LSP ini belum memiliki kerangka kerja pengelolaan risiko yang kuat dan terintegrasi.
2. Fokus Peningkatan
   Berdasarkan status penerapan, LSP dengan nilai lebih rendah secara spesifik perlu beralih dari fase "Dalam Perencanaan" ke "Dalam Penerapan atau Diterapkan Sebagian" atau bahkan "Diterapkan Secara Menyeluruh". Area yang perlu diprioritaskan meliputi:
   a. Pengembangan program kerja dan kerangka kerja pengelolaan risiko yang terdokumentasi dan resmi.
   b. Penetapan ambang batas risiko yang dapat diterima.
   c. Identifikasi ancaman, kelemahan, dan dampak kerugian secara menyeluruh.
   d. Pelaksanaan analisis kajian risiko secara terstruktur.
   e. Implementasi langkah mitigasi dan pemantauan status penyelesaiannya.
   f. Kajian ulang profil risiko secara berkala
   g. Pengembangan kebijakan dan prosedur terkait UU PDP, khususnya mengenai kerahasiaan dan retensi data pribadi.

E. Pelindungan Data Pribadi

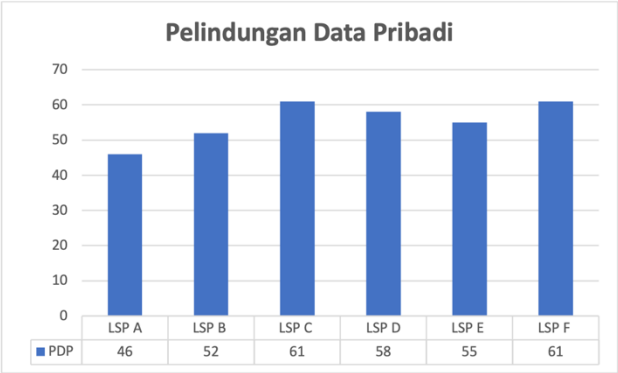
Penilaian komprehensif terhadap tingkat kematangan keamanan informasi di Lembaga Sertifikasi Profesi (LSP), khususnya dalam domain pengelolaan risiko dan perlindungan data pribadi (PDP), menunjukkan variasi signifikan dalam implementasi kewajiban UU PDP. LSP diwajibkan oleh Pasal 36 UU PDP untuk menjaga kerahasiaan data pribadi melalui kebijakan tertulis formal dan prosedur operasional yang mencakup definisi, batasan akses, dan tanggung jawab, guna mencegah dampak pelanggaran yang serius. Sejalan dengan itu, Pasal 42 UU PDP mengatur masa retensi data pribadi, mengharuskan LSP memiliki kebijakan dan prosedur untuk menghapus atau memusnahkan data secara aman setelah tujuan pemrosesan tercapai atau masa retensi berakhir, guna memitigasi risiko penyimpanan data yang tidak perlu. Lebih lanjut, kepatuhan terhadap Pasal 16 UU PDP menuntut transparansi dalam pengumpulan data pribadi peserta melalui kebijakan tertulis dan SOP yang jelas mengenai pengolahan, analisis, serta retensi data. Jika data dikumpulkan di area publik, Pasal 17 UU PDP mewajibkan LSP memiliki kebijakan terkait pemasangan alat visual (misalnya CCTV) yang jelas tujuannya, disertai informasi pemberitahuan visual, dan memiliki kebijakan pengecualian untuk pencegahan tindak pidana atau penegakan hukum. Terakhir, Pasal 46 UU PDP mengharuskan LSP memiliki kebijakan dan prosedur yang formal serta tersosialisasi untuk penanganan kebocoran data pribadi, termasuk pemberitahuan kepada subjek data dan masyarakat umum jika diperlukan, serta menyusun dan mengevaluasi rencana mitigasi risiko secara berkala untuk melindungi dari akses tidak sah, kehilangan, atau perusakan data. Secara keseluruhan, LSP dengan tingkat kematangan rendah pada domain-domain ini menunjukkan kebutuhan mendesak untuk mengembangkan dan mengimplementasikan kerangka kerja risiko yang kuat dan terintegrasi, serta mengoptimalkan proses

inti PDP sesuai amanat UU PDP, dengan memanfaatkan kekuatan yang ada pada tata kelola keamanan informasi yang sudah relatif matang, dengan penambahan 12 pertanyaan baru yang selaras dengan UU PDP Pasal 16, 17, dan 46.

Tabel E-1 Irisan PDP dengan UU PDP

#			UU PDP Pasal 16	
7.17	II	2	Apakah LSP memiliki kebijakan tertulis mengenai proses pengumpulan data pribadi peserta?	
7.18	II	2	Apakah terdapat kebijakan atau SOP terkait proses pengolahan dan analisis data pribadi?	
7.19	II	2	Apakah terdapat kebijakan retensi data yang jelas?	
#			UU PDP Pasal 17	
7.20	II	2	Apakah LSP memiliki kebijakan terkait pemasangan alat pemroses atau pengolah data visual di area publik?	
7.21	III	2	Apakah terdapat informasi yang ditampilkan pada area yang dipasang alat pengolah data visual?	
7.22	III	2	Apakah tujuan pemasangan alat pengolah data visual telah dijelaskan dengan jelas?	
7.23	III	2	Apakah terdapat kebijakan pengecualian untuk pemasangan alat pengolah data visual dalam hal pencegahan tindak pidana?	
7.24	III	2	Apakah terdapat kebijakan tertulis mengenai pengecualian pemasangan alat visual untuk proses penegakan hukum?	
#			UU PDP Pasal 46	
7.25	III	2	Apakah LSP memiliki kebijakan tertulis terkait penanganan kebocoran data pribadi?	
7.26	III	2	Apakah LSP memiliki kebijakan khusus untuk memberitahukan kebocoran data kepada masyarakat umum jika diperlukan?	
7.27	III	2	Apakah LSP telah memiliki kebijakan dan prosedur tertulis yang mengatur pelindungan terhadap akses tidak sah, kehilangan, atau perusakan data pribadi, serta sudah disosialisasikan kepada seluruh pihak terkait ?	
7.28	III	2	Apakah LSP telah menyusun dan mengimplementasikan rencana mitigasi risiko terhadap insiden keamanan data pribadi, serta melakukan evaluasi berkala atas efektivitas pengamanan tersebut ?	
			Total Nilai Evaluasi Pelindungan Data Pribadi	

Penilaian domain pelindungan data pribadi dilakukan untuk mengevaluasi sejauh mana suatu LSP telah mengimplementasikan kebijakan, prosedur, dan mekanisme untuk melindungi data pribadi sesuai dengan peraturan perundang-undangan yang berlaku, termasuk hak-hak subjek data dan penanganan insiden. Domain ini memiliki skor maksimum sebesar 84 poin.

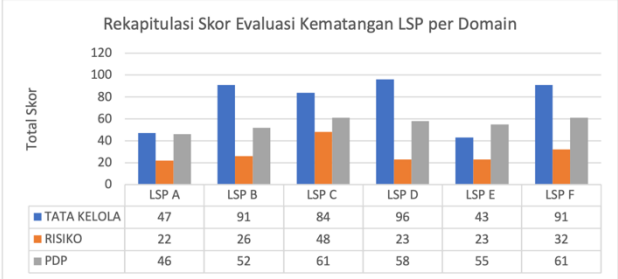


Gambar III-3 Grafik Pelindungan Data Pribadi

Analisis kesiapan implementasi perlindungan data pribadi (PDP) di enam Lembaga Sertifikasi Profesi (LSP) menunjukkan spektrum yang bervariasi. LSP C dan LSP F menunjukkan kesiapan tinggi, berhasil mengimplementasikan mayoritas aspek PDP secara menyeluruh atau sebagian, termasuk program peningkatan pemahaman pegawai dan kebijakan terkait pengolahan data visual di area publik. Sementara itu, LSP D dan LSP E berada pada tingkat menengah, dengan banyak praktik kunci telah diterapkan, terutama pada aspek fundamental seperti pendokumentasian proses pengolahan dan penanganan hak subjek data, meskipun masih ada area yang dalam perencanaan. Sebaliknya, LSP A dan LSP B menunjukkan tingkat kesiapan rendah, dengan sebagian besar elemen penting PDP masih dalam tahap perencanaan, termasuk pengembangan kebijakan lengkap, penunjukan pejabat PDP, program kesadaran pegawai, serta prosedur terkait pengolahan, retensi, dan penanganan kebocoran data pribadi. Secara umum, kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) menjadi fokus utama, dan LSP dengan skor rendah perlu memprioritaskan pengembangan kebijakan dan prosedur PDP yang jelas, penunjukan pejabat yang bertanggung jawab, peningkatan kesadaran pegawai, serta implementasi prosedur yang lebih rinci untuk pengumpulan, pengolahan, retensi, dan penanganan insiden data pribadi.

F. Analisis Gap

Analisis gap dilakukan untuk mengidentifikasi kesenjangan signifikan antara kondisi tata kelola keamanan data pribadi aktual pada LSP dengan standar ideal Indeks KAMI versi 5.0 dan ketentuan UU No. 27 Tahun 2022.



Gambar III-4 Grafik Analisis Gap

Analisis tingkat kematangan Lembaga Sertifikasi Profesi (LSP) menunjukkan kesenjangan signifikan, terutama pada domain Pengelolaan Risiko Keamanan Informasi. Sebagian besar LSP memiliki sistem, proses, dan budaya pengelolaan risiko yang lemah, membuat mereka rentan terhadap berbagai jenis risiko. Kekuatan relatif ditemukan pada domain Tata Kelola Keamanan Informasi, yang dapat menjadi fondasi perbaikan di domain lain. Domain Pelindungan Data Pribadi (PDP) memiliki dasar yang sudah ada tetapi masih memerlukan optimalisasi. Profil kesenjangan bervariasi antar-LSP, dengan beberapa menunjukkan perbedaan besar antara Tata Kelola yang kuat dan Risiko yang lemah, sementara yang lain memiliki Tata Kelola yang juga rendah. Prioritas utama adalah mengatasi kelemahan sistemik dalam manajemen risiko dan mengoptimalkan PDP, dengan memanfaatkan kekuatan Tata Kelola sebagai landasan.

G. Matriks Prioritas

Skala ini dirancang untuk menjadi pedoman strategis dalam mengarahkan alokasi sumber daya dan memfokuskan upaya peningkatan kematangan keamanan informasi. Dengan mengidentifikasi kesenjangan signifikan pada tingkat kematangan dan validitas implementasi SOP, prioritisasi yang disajikan ini berfungsi sebagai basis empiris untuk pengembangan dan implementasi SOP yang paling mendesak dan relevan bagi setiap LSP.

Tabel G-1 Irisan Pengelolaan Risiko dengan UU PDP

LSP	Prioritas Tata Kelola	Prioritas Pengelolaan Risiko	Prioritas Pelindungan Data Pribadi
LSP E	Tinggi (I+, Tidak Valid)	Tinggi (I+, Tidak Valid)	Tinggi (I+, Tidak Valid)
LSP A	Tinggi (I+, Tidak Valid)	Tinggi (I+, Tidak Valid)	Tinggi (II, Tidak Valid)
LSP F	Rendah (II, Valid)	Tinggi (I+, Tidak Valid)	Tinggi (I+, Tidak Valid)
LSP B	Rendah (II, Valid)	Tinggi (I+, Tidak Valid)	Tinggi (II, Tidak Valid)
LSP D	Rendah (II, Valid)	Tinggi (I+, Tidak Valid)	Tinggi (II, Tidak Valid)
LSP C	Rendah (II+, Valid)	Tinggi (II, Tidak Valid)	Tinggi (II+, Tidak Valid)

Kematangan suatu area dinilai berdasarkan dua kriteria: Tingkat Kematangan (T. Kematangan) dan validitas tahap implementasi 3. Tingkat kematangan bervariasi dari dasar (I+) hingga tertinggi (II+). Status "Tidak Valid" pada tahap implementasi 3 menunjukkan perlunya pengembangan atau perbaikan Standar Operasional Prosedur (SOP) yang mendesak, terutama untuk tingkat kematangan I+ dan II. Sebaliknya, status "Valid" pada tahap implementasi 3, khususnya untuk tingkat kematangan II dan II+, mengindikasikan bahwa kebutuhan SOP sudah terpenuhi dengan baik dan tidak memerlukan prioritas tinggi untuk perbaikan.

Berikut adalah daftar SOP untuk setiap Lembaga Sertifikasi Profesi, berdasarkan kesenjangan kunci terpenting yang teridentifikasi dari evaluasi Indeks KAMI. Prioritasi ini berfokus pada Langkah-langkah yang paling mendasar dan berdampak besar untuk peningkatan awal.

Tabel G-2 Daftar Kebutuhan SOP per LSP

No	SOP	LSP A	LSP B	LSP C	LSP D	LSP E	LSP F
1	Perencanaan dan Penetapan Kebijakan Keamanan Data Pribadi						
2	Penunjukan dan Penetapan Petugas Pelindungan Data Pribadi (DPO)						
3	Pengumpulan dan Persetujuan Data Pribadi						
4	Penyimpanan dan Pengamanan Data Pribadi						
5	Pengelolaan Hak Subjek Data Pribadi						
6	Pengelolaan Risiko keamanan Data Pribadi						
7	Penangan Insiden Keamanan Data Pribadi						
8	Peningkatan Kompetensi dan Kesadaran Keamanan Data Pribadi						
9	Audit dan Evaluasi Tata Kelola Keamanan Data Pribadi						

IV. Simpulan

Hasil penilaian menunjukkan bahwa tata kelola keamanan data pribadi di LSP masih berada pada kategori "Cukup", yang berarti belum memenuhi standar kelengkapan dan kematangan optimal. Aspek seperti kebijakan formal, pembagian tanggung jawab, dan mekanisme audit masih belum terdokumentasi dengan baik. Secara spesifik, domain Risiko dan Pelindungan Data Pribadi (PDP) merupakan aspek terlemah dalam dokumentasi dan implementasi, meskipun domain Tata Kelola menunjukkan tingkat kematangan tertinggi. Hal ini mengindikasikan bahwa LSP memiliki mekanisme dasar, namun belum menerapkan pendekatan yang sistematis dan berkelanjutan dalam pelindungan data.

Penelitian ini mengidentifikasi 27 indikator dalam Indeks KAMI yang selaras dengan pasal-pasal utama UU PDP (Pasal 16, 17, 20, 33, 35, 46, dan juga Pasal 5-14 serta Pasal 53). Keselarasan ini mencakup tiga domain: Tata Kelola, Risiko, dan Pelindungan Data Pribadi. Pemetaan ini membentuk struktur matriks yang bermanfaat bagi LSP untuk mengidentifikasi area kesesuaian, kekosongan, dan peluang perbaikan kebijakan internal demi mencapai kepatuhan terhadap regulasi nasional.

Sebagai respons terhadap temuan ini, penelitian merekomendasikan sembilan Standar Operasional Prosedur (SOP) utama untuk mendukung peningkatan tata kelola keamanan data pribadi di LSP. Rekomendasi SOP ini meliputi kebijakan, penunjukan Petugas Pelindungan Data (DPO), pengelolaan hak subjek data, peningkatan kompetensi, serta audit dan evaluasi. SOP ini dirancang berdasarkan prinsip tata kelola TI, indikator Indeks KAMI, dan ketentuan UU PDP, menjadikannya acuan implementatif untuk meningkatkan kepatuhan dan efektivitas pelindungan data di LSP.

Referensi

[1] Lembaga Sertifikasi Profesi (LSP), data diperoleh melalui situs internet: https://jdih.kemenkeu.go.id/kamus-hukum/lembaga-sertifikasi-profesi?id=02c4b81e52d95931825b77ecb018c457, Diakses pada tanggal 21 Maret 2025 pukul 14.02 WIB.

[2] Pilo R, (2023), Pelindungan Data Pribadi: Pentingnya Keamanan Informasi Pada Bisnis Modern, Phintraco Group, https://phintraco.com/pelindungan-data-pribadi/, Diakses pada tanggal 21 Maret 2025 pukul 14.15 WIB.

[3] Saputra C Deannova, Saputra G Septiawan, dkk, (2024), Perspektif Hukum terhadap Privasi dan Pelindungan Data Pribadi di Era Digital, Jurnal Ilmu Hukum, Humaniora dan Politik (JIHHP), Vol. 5 No. 1, Diakses pada tanggal 21 Maret 2025 pukul 14.30 WIB.

[4] Christian D, (2022), UU PDP: Landasan Hukum Pelindungan Data Pribadi, Hukum Online, https://www.hukumonline.com/klinik/a/uu-pdp--landasan-hukum-pelindungan-data-pribadi-lt5d588c1cc649e/, Diakses pada tanggal 21 Maret 2025 pukul 15.00 WIB.

[5] Badan Sandi Siber Negara (BSSN), data diperoleh melalui internet: https://www.bssn.go.id/?s=indeks+kami&et_pb_searchform_submit=et_search_proccess&et_pb_include_posts=yes&et_pb_include_pages=yes, Diakses pada tanggal 21 Maret 2025 pukul 15.08 WIB.

[6] Badan Sandi Siber Negara (BSSN), (2021), Pedoman Indeks Keamanan Informasi (Indeks Kami), Diakses pada tanggal 03 April 2025 pukul 23.10 WIB

[7] Pratiwi A Hadiati dan Wulandari Lily, (2019), Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor, Journal of Industrial Engineering & Management Research (JIEMAR), Vol. 2 No. 5, Diakses pada tanggal 21 Maret 2025 pukul 15.20 WIB.

[8] Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Sekretariat Negara. Jakarta.

[9] Chaesya A Dwi, (2021), Evaluasi Manajemen Terhadap Keamanan Informasi Dengan Menggunakan Indeks KAMI Pada BPR Fianka Rezalina Fatma, Skripsi, UIN SUSKA RIAU, Fakultas Sains dan Teknologi. Diakses pada tanggal 8 Februari 2025 pukul 17.43 WIB.

[10] Mohammed A Mahammed, Al-Abedi K Thamer, dkk (2021), Internal Control Frameworks and Its Relation with Governance and Risk Management: AN Analytical Study, Estudios de Economia Aplicada, Vol. 39 No. 11, Diakses pada tanggal 12 April 2025 pukul 18.47 WIB.

[11] Hasanah I Nida, (2024), Strategi Membangun Tata Kelola Pemerintahan Yang Baik Mellaui Pengembangan Manajemen Risiko, data diperoleh melalui situs internet : https://inspektorat.lebakkab.go.id/berita/detail/strategi-membangun-tata-kelola-pemerintahan-yang-baik-melalui-pengembangan-manajemen-risiko, Diakses pada tanggal 12 April 2025 pukul 18.50 WIB.

[12] Kemnaker, 2024, Lembaga Sertifikasi Profesi (LSP) Terlisensi Semester II Tahun 2023, data diperoleh melalui situs internet : https://satudata.kemnaker.go.id/data/kumpulan-data/1718, Diakses pada tanggal 13 April 2025 pukul 17.05 WIB.

[13] Microsoft (2025), Tata Kelola Data, data diperoleh melalui situs internet : https://www.microsoft.com/id-id/security/business/security-101/what-is-data-governance-for-enterprise, Diakses pada tanggal 13 April 2025 pukul 17.30 WIB.

[14] Hidayah A, (2023), 5 (Lima) Prinsip Good Governance dalam Pengurusan Piutang Negara, Artikel DJKN, Diakses pada tanggal 19 Mei 2025 pukul 21.20 WIB.

[15] Badan Nasional Sertifikasi Profesi (BNSP), data diperoleh melalui situ sinternet : https://bnsp.go.id/, Diakses pada tanggal 19 Mei 2025 pukul 21.35 WIB.
[16] Kennedy A, (2024), Perlindungan Data Pribadi Dalam Dunia Siber di Indonesia Ditinjau Berdasarkan Hukum Tata Negara, Jurnal Pedia, Vol. 06 No. 2, Diakses pada tanggal 20 Mei 2025 pukul 08.05 WIB.
[17] ISO/IEC 27001, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Diakses pada tanggal 20 Mei 2025 pukul 08.14 WIB.
[18] Peraturan Pemerintah No. 10 Tentang Badan Nasional Sertifikasi Profesi Tahun 2018, Diakses pada tanggal 20 Mei 2025 pukul 08.31 WIB.