BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi dan pengujian sistem analisis risiko privasi (*PRISMA COKRO GEN 1.0 (BETA)*) yang telah dilakukan, dapat ditarik beberapa kesimpulan sebagai berikut:

a. Perancangan *Framework* Terintegrasi (*Hybrid Model*)

Penelitian ini berhasil menjawab tantangan penggabungan metode kuantitatif dengan standar regulasi melalui pengembangan kerangka kerja hibrida. Sistem menerjemahkan prinsip abstrak UU PDP 2022 Tahun 2022 (khususnya sensitivitas data pada Pasal 4) menjadi bobot variabel *Impact* dan kontrol keamanan *NIST CSF 2.0* menjadi bobot variabel *Likelihood*. Hasilnya adalah sebuah algoritma deterministik yang mampu menilai risiko privasi bukan hanya berdasarkan probabilitas teknis, tetapi juga konteks kepatuhan hukum yang berlaku di Indonesia.

b. Implementasi Sistem Web Statis Berbasis Parameter Teknis

Framework ini diimplementasikan sebagai web statis *PRISMA COKRO GEN 1.0 (BETA)* yang berjalan sepenuhnya *client-side*. Seluruh pemrosesan parameter serta modul *Risk Engine* dan *Legal Engine* dilakukan di *browser* tanpa pengiriman data ke *server*, sehingga memenuhi prinsip *zero-knowledge*, *Privacy by Design* dan *Data Minimization*. Sistem juga menyediakan *encrypted local persistence* untuk menyimpan progres secara lokal serta fitur email *feedback* untuk pemeliharaan *registry* tanpa mengekspos data sensitif, sehingga efektif sebagai solusi otomatisasi penilaian risiko yang aman dan mendukung asesmen mandiri.

c. Konsistensi Penilaian Risiko, Kepatuhan dan Rekomendasi

Berdasarkan pengujian terhadap tiga skenario berbeda, sistem terbukti mampu menghasilkan penilaian risiko, status kepatuhan dan rekomendasi mitigasi yang konsisten dan kontekstual melalui tiga jalur logika yaitu Mekanisme *Institutional Trust Override*, Mekanisme Penalti Ilegal dan Kalkulasi Standar Objektif

5.2 Saran

Berdasarkan keterbatasan sistem yang ada saat ini dan potensi pengembangan teknologi di masa depan, berikut adalah beberapa saran untuk pengembangan penelitian selanjutnya:

a. Transisi dari *Hardcoded Registry* ke *API* yang Terintegrasi

Sistem saat ini masih mengandalkan basis data statis (*array*) untuk validasi legalitas. Pengembangan selanjutnya diharapkan dapat mengintegrasikan API publik dari regulator seperti PSE, OJK atau Kominfo (PSE). Hal ini bertujuan agar sistem dapat memverifikasi status legalitas layanan secara *real-time* tanpa perlu pembaruan kode manual.

b. Peningkatan Integritas Arsitektur Sistem

Mengingat arsitektur saat ini berjalan sepenuhnya di sisi klien (*client-side*), terdapat celah risiko manipulasi variabel skor oleh pengguna yang memiliki kemampuan teknis. Untuk implementasi pada skala industri atau audit formal, disarankan memindahkan logika inti (*Risk Engine*) ke lingkungan *Backend Server* yang aman, atau menerapkan mekanisme *Digital Signature* untuk menjamin integritas kode *JavaScript* yang berjalan.

c. Perluasan Cakupan *Full Profile NIST CSF 2.0*

Penelitian ini membatasi ruang lingkup analisis pada 12 kontrol teknis utama (*Target Profile*). Untuk memperoleh analisis risiko yang lebih holistik, pengembangan selanjutnya disarankan memperluas parameter penilaian menjadi *Full Profile NIST CSF 2.0* (106 sub-kategori), dengan mencakup aspek non-teknis seperti tata kelola, kebijakan organisasi, manajemen risiko dan faktor sumber daya manusia sesuai kerangka kerja penuh *NIST CSF 2.0*.

d. Integrasi *Generative AI*

Saat ini, rekomendasi perbaikan yang dihasilkan sistem bersifat statis berdasarkan teks standar *NIST CSF 2.0*. Pengembangan selanjutnya dapat mengintegrasikan model bahasa besar (*Large Language Model*/LLM) berskala kecil atau API AI untuk menghasilkan saran mitigasi yang lebih kontekstual, dinamis dan mudah dipahami (*human-readable*).