**Sovereign: AI Compliance Violation Predictor – Product Requirements Document (PRD)**

**TL;DR**

**Summary:**  
Sovereign is an AI-powered platform that helps organizations proactively assess GDPR compliance risks in their AI systems. It provides intelligent document analysis, a multi-step compliance workflow, and actionable implementation roadmaps for Data Protection Officers, AI Product Managers, and Compliance Consultants.

**Goals**

**Business Goals**

1. Enable organizations to identify and address GDPR compliance gaps in AI systems.
2. Deliver professional, audit-ready compliance reports.
3. Achieve <10 second analysis response time and 95%+ demo reliability.
4. Demonstrate portfolio-quality work for academic and professional advancement.

**User Goals**

1. Quickly analyze privacy policies and AI system documentation for compliance gaps.
2. Receive actionable, step-by-step implementation plans.
3. Export professional reports for internal or client use.

**Non-Goals**

1. Not intended for commercial deployment or production-scale security.
2. No support for non-GDPR regulatory frameworks.
3. No integration with proprietary or paid compliance tools.

**User Stories**

**Personas & Stories**

**Data Protection Officer (DPO):**

1. As a DPO, I want to upload privacy policies and AI system docs, so I can identify GDPR compliance gaps quickly.
2. As a DPO, I want to receive suggested policy updates, so I can keep our documentation current.

**AI Product Manager:**

1. As an AI PM, I want to assess compliance risks before development, so I can avoid costly rework.
2. As an AI PM, I want a clear implementation plan, so I can prioritize compliance tasks.

**Compliance Consultant:**

1. As a consultant, I want to generate professional audit reports, so I can deliver value to multiple clients.
2. As a consultant, I want to export action items in CSV, so I can integrate them into client workflows.

**Functional Requirements**

**Feature Groups & Priorities**

1. **Document Upload & OCR (High):**
   * Upload PDF/Word files, extract text using OCR.
2. **Multi-Step AI Analysis (High):**
   * 5-step workflow: GDPR → Cross-Reference → Bias → Ethics → Planning.
3. **Cross-Reference Intelligence (Medium):**
   * Compare AI system details with privacy policies.
4. **Implementation Planning (Medium):**
   * Generate step-by-step compliance roadmaps.
5. **Professional Reporting (Medium):**
   * Export PDF reports and CSV action items.
6. **Progress Tracking & Dashboard (Low):**
   * Visualize analysis progress and results.

**User Experience**

**Entry Point & Onboarding**

1. Users access a web app, register/login, and see a dashboard.
2. Onboarding wizard guides first-time users through document upload and system description.

**Core Experience**

1. **Step 1:** Upload privacy policy and AI system documentation.
2. **Step 2:** System extracts and displays text for review.
3. **Step 3:** User describes AI system (form input).
4. **Step 4:** Initiate multi-step analysis; progress bar shows workflow stages.
5. **Step 5:** Results dashboard displays compliance gaps, bias/ethics findings, and implementation plan.
6. **Step 6:** User exports PDF report and CSV action items.

**Advanced Features & Edge Cases**

1. Handle OCR errors and unsupported file types gracefully.
2. Allow users to re-run analysis after updating documents.

**UI/UX Highlights**

1. Clean, professional interface with clear calls to action.
2. Accessibility: high contrast, keyboard navigation, readable fonts.

**Narrative**

A DPO at a fast-growing AI company uploads their privacy policy and AI system documentation into Sovereign. The platform extracts the text, guides them through a multi-step compliance analysis, and highlights gaps between their documentation and actual system practices. Within minutes, the DPO receives a professional report with actionable recommendations, helping the company avoid costly GDPR violations and demonstrating due diligence to stakeholders.

**Success Metrics**

**User-Centric**

1. 90%+ user satisfaction in demo feedback.
2. 80%+ of users able to generate a report without assistance.

**Business**

1. <10 second average analysis time.
2. 95%+ demo reliability (no critical errors during presentations).

**Technical**

1. 95%+ uptime during demo.
2. Support for 10+ concurrent users.

**Tracking Plan**

1. Document uploads, analysis initiations, report exports, error events.

**Technical Considerations**

**Technical Needs**

1. **Frontend:** React app with file upload, progress, and results dashboard.
2. **Backend:** Flask API, OCR (Google Vision), workflow orchestration, SQLite DB.
3. **AI Processing:** Claude API for 5-step analysis.
4. **Export:** PDF and CSV generation.

**Integration Points**

1. Google Vision API (OCR)
2. Claude API (AI analysis)

**Data Storage & Privacy**

1. Store documents and results in SQLite (demo only).
2. Basic file validation and error handling.

**Scalability & Performance**

1. Support 10+ concurrent users.
2. <10 second response time for analysis.

**Potential Challenges**

1. OCR accuracy on complex documents.
2. Managing API rate limits and errors.
3. Ensuring reliability with limited coding experience.

**Milestones & Sequencing**

**Project Estimate**

* **Medium:** 2 weeks (14 days)

**Team Size & Composition**

* 5 AI Product Managers (all roles: PM, dev, QA, design)

**Phase 1: Setup & Core Infrastructure (2 days)**

* Deliverables: Repo setup, Heroku deployment, basic React/Flask skeleton.

**Phase 2: Document Upload & OCR (3 days)**

* Deliverables: File upload UI, OCR integration, text extraction.

**Phase 3: Multi-Step AI Analysis (4 days)**

* Deliverables: Claude API integration, workflow logic, results display.

**Phase 4: Reporting & Export (3 days)**

* Deliverables: PDF/CSV export, professional report formatting.

**Phase 5: Polish & Demo Prep (2 days)**

* Deliverables: UI/UX improvements, error handling, demo script.

**End of Document**