ARRAKIS

U.S. Data Privacy Case Studies: Integrating ISO 27001, ISO 42001, SOC2, and AI Governance

Arrakis Consulting







Purpose

This document presents three practical case studies for organizations navigating U.S. data privacy requirements alongside information security, AI governance, and assurance expectations. Because the United States does not have one comprehensive federal privacy law, organizations must account for applicable state privacy laws, sector-specific rules, contractual obligations, and consumer-protection standards.

The scenarios cross-reference common U.S. privacy requirements, ISO/IEC 27001, ISO/IEC 42001, SOC 2, and relevant AI governance obligations.

Case Study 1: B2B SaaS Company Responds to State Privacy Requirements

Situation

A software-as-a-service provider collected business-contact data, product telemetry, support tickets, and account records from customers across the United States. Growth into California, Colorado, Virginia, Connecticut, and other states exposed inconsistent privacy notices, unclear data-retention practices, and a fragmented process for consumer requests.

Actions Taken

- Created a data inventory identifying personal information, processing purposes, retention periods, sharing practices, and service providers.
- Updated privacy notices to describe collection, use, disclosure, retention, and consumer-rights processes.
- Established workflows for access, deletion, correction, and opt-out requests where required.
- Implemented data minimization, role-based access, multi-factor authentication, encryption, and quarterly access reviews.
- Updated vendor contracts with privacy, security, breach-notification, and subprocessors provisions.

Results

The company created a repeatable privacy operating model that supported sales diligence, customer trust, and audit readiness. It also reduced unnecessary data retention and improved response coordination across legal, engineering, support, and security teams.

Cross-References

- **U.S. privacy laws:** State consumer privacy laws such as the California Consumer Privacy Act and California Privacy Rights Act, Colorado Privacy Act, Virginia Consumer Data Protection Act,

and Connecticut Data Privacy Act may impose notice, consumer-rights, contractual, and opt-out obligations depending on applicability.

- **ISO/IEC 27001:** Risk management, access control, supplier security, asset and information classification, incident management, and documented evidence.
- **SOC 2:** Security and confidentiality criteria support logical access controls, change management, monitoring, vendor oversight, and protection of confidential information.
- **ISO/IEC 42001:** Relevant if analytics, profiling, or automated systems use personal information; supports governance, impact assessment, transparency, and lifecycle management.
- **AI governance:** Evaluate whether automated decision-making, profiling, or high-impact uses create additional state-law, contractual, or consumer-protection risk.

Case Study 2: Healthcare Organization Governs AI-Assisted Patient Triage

Situation

A healthcare organization implemented an AI-assisted triage tool to help prioritize patient-submitted symptoms. The service processed protected health information and could affect how quickly patients were routed for clinical review.

Actions Taken

- Conducted a privacy and security risk assessment before deployment.
- Defined the AI system's intended use, known limitations, human-review process, escalation criteria, and accountability owners.
- Enforced minimum-necessary data practices and restricted access to authorized personnel.
- Performed vendor due diligence covering data use, security safeguards, model monitoring, retention, and subcontractors.
- Implemented audit logging, performance testing, bias monitoring, clinician override controls, and incident-response procedures.

Results

The organization preserved clinical decision authority, strengthened safeguards for sensitive information, and documented governance evidence for customers, regulators, and business partners.

Cross-References

- **U.S. privacy laws:** HIPAA Privacy, Security, and Breach Notification Rules apply to covered entities and business associates handling protected health information. Certain state health-data laws may impose additional obligations.
- **ISO/IEC 27001:** Information security risk assessment, secure development, access management, operational monitoring, supplier assurance, and incident response.

- **SOC 2:** Security, availability, confidentiality, processing integrity, and privacy criteria can support controls over systems processing sensitive healthcare information.
- **ISO/IEC 42001:** AI management system controls for impact assessment, data governance, transparency, human oversight, monitoring, performance evaluation, and continual improvement.
- **AI governance:** Document human oversight, validation, explainability appropriate to the use case, and processes for detecting and correcting harmful or inaccurate outputs.

Case Study 3: Retailer Uses Generative AI in Customer Support

Situation

A national retailer introduced a generative-AI assistant to draft responses to customer questions about orders, returns, and product availability. Employees occasionally entered order information and customer complaint histories into the tool without an approved process for data handling or output review.

Actions Taken

- Defined approved AI use cases and prohibited unnecessary entry of personal, payment-card, or sensitive information.
- Added human review and escalation requirements for refunds, complaints, account actions, and sensitive customer interactions.
- Completed vendor due diligence covering data location, retention, training-data use, security controls, subprocessors, and breach notifications.
- Updated AI-use, data-classification, acceptable-use, and incident-response policies.
- Added customer-facing disclosures and monitored outputs for inaccurate, harmful, or misleading content.

Results

The retailer retained efficiency benefits while reducing the likelihood of data leakage, inconsistent service, misleading communications, and ungoverned AI expansion.

Cross-References

- **U.S. privacy laws:** Applicable state privacy laws may require notice, consumer-rights handling, opt-out mechanisms for certain sharing or targeted advertising, and contractual controls with service providers. FTC consumer-protection authority may also apply to deceptive or unfair privacy and AI practices.
- **ISO/IEC 27001:** Data classification, access control, secure configuration, supplier security, monitoring, and incident management.

- **SOC 2:** Security and confidentiality controls support approved-use restrictions, logical access, vendor governance, monitoring, and evidence of control operation. Privacy criteria can support notice and personal-information handling practices.
- **ISO/IEC 42001:** AI policy, accountability, system inventory, impact assessment, data governance, transparency, performance evaluation, and corrective action.
- **AI governance:** Assess automated-decision risks, model limitations, consumer disclosures, testing, human review, and documentation before scaling use cases.

Implementation Takeaways

- Build one inventory covering personal information, sensitive data, systems, vendors, and AI use cases.
- Determine which state and sector-specific rules apply based on data, geography, revenue, volume, and business role.
- Align privacy requirements with the ISO/IEC 27001 information security management system, ISO/IEC 42001 AI management system, and SOC 2 control environment.
- Use documented risk assessments, vendor reviews, policies, access reviews, monitoring, and incident exercises as shared evidence across frameworks.
- Maintain clear ownership between legal, privacy, security, engineering, operations, and executive leadership.

Conclusion

U.S. privacy compliance requires a practical, layered approach. State privacy statutes, HIPAA and other sector rules, FTC expectations, contracts, and emerging AI obligations must be assessed together. Integrating those obligations with ISO/IEC 27001, ISO/IEC 42001, and SOC 2 reduces duplicated effort, strengthens evidence for customers and auditors, and enables responsible use of data and AI.

.

Ready to get started?

Reach out to use at your earliest convenience to get your company closer to compliance, pass a certifying audit, reduce risk, or increase the skillsets of your personnel.

sales@arrakisconsulting.com

www.arrakisconsulting.com

Arrakis Consulting, LLC