ARRAKIS

Arrakis Consulting

GDPR Case Studies: Integrating ISO 27001, ISO 42001, and the EU AI Act

Purpose

This document presents three practical GDPR case studies for organizations managing information security, artificial intelligence, and European regulatory obligations. Each example highlights the operational issue, compliance response, measurable outcome, and relevant cross-references to ISO/IEC 27001, ISO/IEC 42001, and the EU AI Act.

Case Study 1: SaaS Provider Strengthens Lawful Processing and Security

Situation

A B2B SaaS company serving European customers processed customer contact data, usage analytics, and support records across multiple cloud platforms. Its privacy notice and vendor agreements had not kept pace with product growth, and access permissions were inconsistent across teams.

Actions Taken

- Mapped personal-data flows, purposes, retention periods, and processors.
- Updated privacy notices, data-processing agreements, and records of processing activities.
- Implemented role-based access control, multi-factor authentication, encryption, and quarterly access reviews.
- Established a data-subject request procedure for access, deletion, correction, and portability requests.
- Created an incident response workflow with breach-assessment and notification decision points.

Results

The company improved its ability to demonstrate accountability, reduced unnecessary access to personal data, and shortened data-subject request response times. It also created a repeatable evidence set for customer due diligence.

Cross-References

- **GDPR:** Articles 5, 6, 25, 28, 30, 32, 33, and 34.
- **ISO/IEC 27001:** Information security management, risk treatment, access control, supplier security, incident management, and documented evidence.
- **ISO/IEC 42001:** Useful where automated analytics or AI features influence personal-data processing; supports governance, impact assessment, transparency, and lifecycle controls.
- **EU AI Act:** If the platform includes AI functionality, classify the system, document intended purpose, maintain technical documentation, and apply transparency obligations where applicable.

Case Study 2: Healthcare Organization Deploys AI-Assisted Triage

Situation

A healthcare organization introduced an AI-assisted triage tool that analyzed patient-submitted symptoms to prioritize clinical review. The solution handled special-category health data and could materially influence how quickly patients received attention.

Actions Taken

- Conducted a Data Protection Impact Assessment before deployment.
- Defined the system's intended use, performance limits, human-review requirements, and escalation process.
- Minimized data inputs and separated identifying information from model-development datasets where practical.
- Implemented bias testing, performance monitoring, audit logs, and clinician override controls.
- Trained staff to explain the tool's role and report suspected errors or harmful outcomes.

Results

The organization deployed the tool with clearer accountability, stronger safeguards for sensitive data, and documented human oversight. Clinical teams retained final decision authority, reducing the risk of unchecked automated decision-making.

Cross-References

- **GDPR:** Articles 5, 9, 22, 25, 32, and 35; health data requires heightened safeguards, and solely automated decisions require careful review.
- **ISO/IEC 27001:** Risk assessment, secure system development, access management, logging, supplier assurance, and incident handling.
- **ISO/IEC 42001:** AI management system, impact assessments, data governance, transparency, human oversight, monitoring, and continual improvement.
- **EU AI Act:** AI used in healthcare may be high-risk depending on its purpose and context. Requirements may include risk management, data governance, technical documentation, logging, human oversight, accuracy, robustness, and cybersecurity.

Case Study 3: Retailer Uses Generative AI for Customer Support

Situation

A retailer deployed a generative-AI assistant to draft responses to customer inquiries. Early testing showed that employees sometimes pasted order details and complaint histories into the tool without a clear approval process or retention controls.

Actions Taken

- Limited approved use cases and prohibited entry of unnecessary personal or payment data.
- Performed vendor due diligence covering data location, subprocessors, training-data use, retention, security controls, and contractual commitments.
- Added human review for customer-facing responses and an escalation path for complaints, refunds, and sensitive requests.
- Updated internal AI-use policies, training, and monitoring procedures.
- Added disclosures so customers understood when they were interacting with an AI-enabled service.

Results

The retailer retained productivity benefits while reducing the likelihood of unauthorized disclosure, inaccurate responses, and inconsistent customer treatment. The organization gained a governed process it could expand across other AI use cases.

Cross-References

- **GDPR:** Articles 5, 6, 13–14, 25, 28, 32, and 44–49 where international transfers apply.
- **ISO/IEC 27001:** Supplier relationships, asset and data classification, access control, secure configuration, monitoring, and incident response.
- **ISO/IEC 42001:** AI policy, accountability, AI system inventory, impact assessment, transparency, data governance, and performance evaluation.
- **EU AI Act:** General-purpose AI and transparency requirements may apply depending on the model, deployment, and user-facing design. Clearly communicate AI interaction where required and maintain appropriate governance documentation.

Implementation Takeaways

- Treat privacy, security, and AI governance as one operating model—not separate projects.
- Begin with a complete data and AI-system inventory.
- Use risk assessments and impact assessments to prioritize controls and evidence.
- Keep human accountability in decisions that affect individuals.
- Document policies, assessments, vendor reviews, testing, incidents, and corrective actions.

Conclusion

GDPR compliance is strengthened when organizations connect privacy obligations with an ISO/IEC 27001 information security management system and an ISO/IEC 42001 AI management system. The EU AI Act adds a further governance layer for AI systems, particularly where risk, transparency, human oversight, and technical documentation are central. A unified approach reduces duplication, improves audit readiness, and supports responsible innovation.

.

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