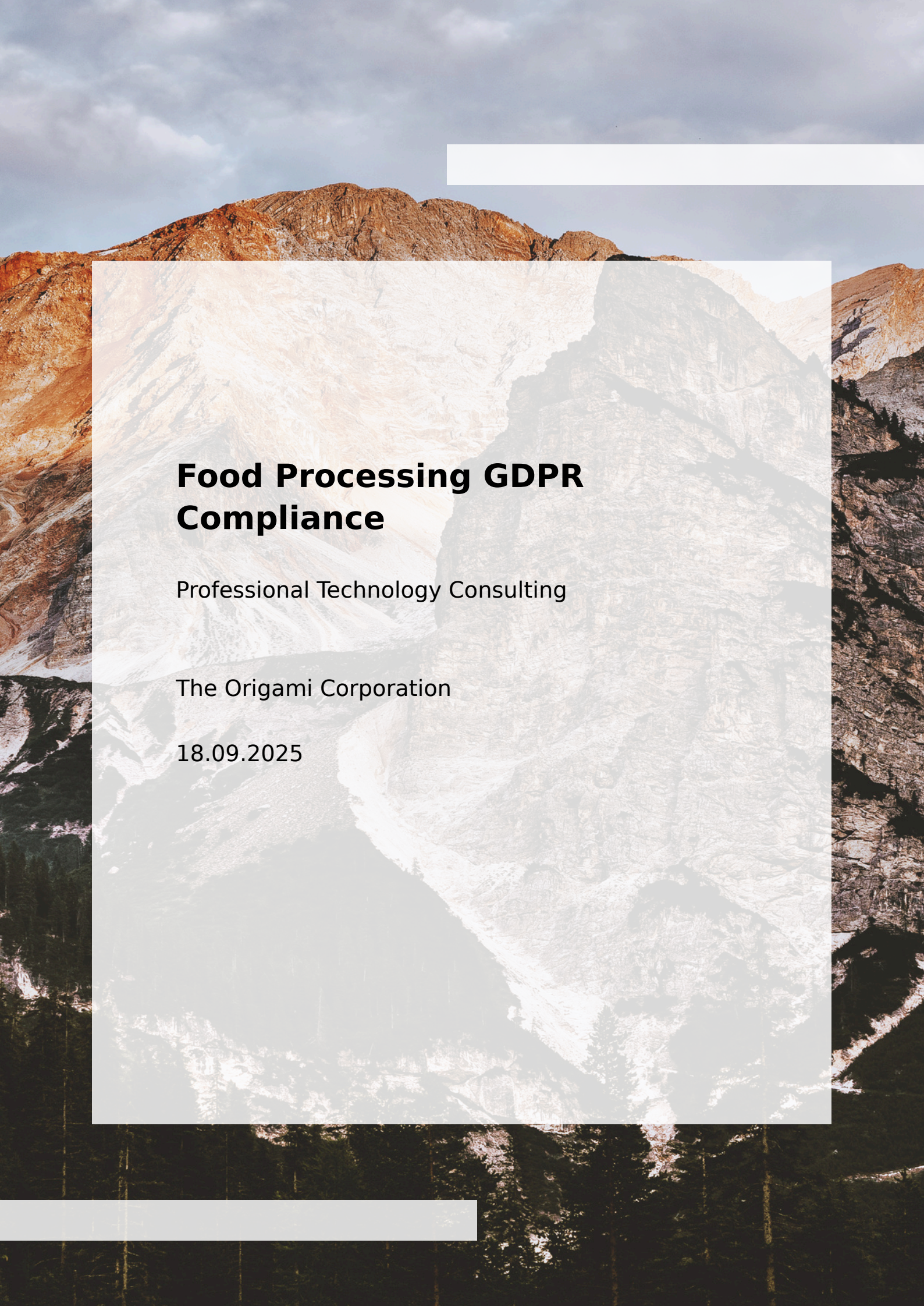




Food Processing GDPR Compliance

Professional Technology Consulting

The Origami Corporation

18.09.2025

Table of Contents

1 From Regulatory Risk to Operational Resilience: Accelerating GDPR Compliance for a Pan-EU Food Processor

1.1 Executive Summary

1.2 The Challenge

1.3 Our Approach

1.4 Implementation

1.5 Results & Impact

1.6 Technologies & Services Used

1.7 Conclusion

About The Origami Corporation

1

1

1

2

2

4

4

5

1 From Regulatory Risk to Operational Resilience: Accelerating GDPR Compliance for a Pan-EU Food Processor

1.1 Executive Summary

A mid-sized food processing company operating across five EU countries received regulator warnings for GDPR non-compliance. Fragmented data across HR, customer, and supplier systems, inconsistent consent tracking, and manual subject rights handling placed them at elevated legal and operational risk. We executed a rapid compliance-audit-gdpr, deployed security-hardening across identity, data, and infrastructure layers, implemented our Origami ERP to centralize data governance, optimized core privacy-related business processes, and delivered targeted security-awareness-training to 120 employees. Within four months, the client achieved full GDPR compliance, avoided up to €2M in potential fines, and realized measurable operational gains, including saving 15 hours per week on data subject requests.

1.2 The Challenge

The client’s growth across multiple EU jurisdictions had outpaced governance structures:

- Disparate systems: HR databases, regional CRM instances, and supplier portals replicated personal data across countries with no unified Records of Processing Activities (RoPA).

- Manual privacy operations: Data Subject Access Requests (DSARs) were handled via email and spreadsheets, leading to inconsistent responses and missed internal deadlines.
- Policy and control gaps: Retention schedules were incomplete; lawful basis for certain processing activities was undocumented; vendor DPAs and SCCs were inconsistent; and technical controls did not demonstrably meet Article 32 standards.
- Limited visibility: No centralized inventory of personal data, weak audit trails, and no systematic DPIA trigger process for new initiatives.

The regulator's warning created a tight timeline to demonstrate remediation and sustainable compliance.

1.3 Our Approach

We applied an integrated program combining five services:

- compliance-audit-gdpr to establish an authoritative RoPA, identify gaps against GDPR Articles 5, 6, 13/14, 17, 20, 28, 30, 32, and 35, and define a prioritized remediation plan.
- security-hardening to uplift identity, data, and infrastructure controls and produce defensible evidence of security of processing.
- erp-implementation of Origami ERP to centralize master data, enforce retention and access controls, and provide auditable workflows for subject rights.
- business-process-optimization to streamline DSARs, incident response, consent management, and vendor onboarding with clear SLAs and ownership.
- security-awareness-training tailored by role to convert policy into daily practice and reduce human risk.

Our methodology was executed in four sprints over 16 weeks: Discover, Design, Implement, and Validate.

1.4 Implementation

Phase 1: GDPR Compliance Audit and Data Mapping - Stakeholder interviews across HR, Sales/Customer Service, Procurement, IT, and Legal in five countries. - Built a consolidated RoPA covering 64 processing activities; identified 11 high-risk activities requiring DPIAs. - Ran automated data discovery across databases and shared drives; tagged PII and special categories; established data lineage into and out of HRIS, CRM, and supplier systems. - Gap analysis revealed deficiencies in lawful basis documentation for recruitment and marketing communications, retention rules for supplier contacts, incomplete privacy notices, and ad hoc DSAR handling. - Drafted and approved updated privacy notices (multilingual), a GDPR-aligned retention schedule, DSAR SOPs, an incident response playbook, and a vendor due

diligence checklist. Executed standardized DPAs and SCCs with 18 processors; established a formal TIA template for data transfers.

Phase 2: Security Hardening - Identity and access: Implemented SSO using OIDC across Origami ERP and connected apps; enforced MFA for all privileged accounts and high-risk roles; introduced role-based access control (RBAC) aligned to least privilege; quarterly access review cadence established. - Data protection: Enabled AES-256 encryption at rest and TLS 1.2+ in transit; deployed field-level encryption for national identifiers; pseudonymized datasets used for analytics; configured European data residency for all backups and archives with immutable snapshots and tested restorations. - Infrastructure and endpoints: Applied CIS Level 1 hardening baselines; instituted a 14-day patching SLA for critical vulnerabilities; rolled out EDR on endpoints accessing ERP; segmented ERP and HR networks; implemented secure file transfer for supplier documents. - Monitoring and auditability: Centralized logging with immutable audit trails (12-month retention); alerting for anomalous access; monthly vulnerability scans and remediation reporting tied to Article 32 evidence.

Phase 3: Origami ERP Implementation - Deployed Origami ERP modules for HR, Supplier Management, and Customer & Order Management to centralize personal data and master records. Consolidated nine disparate data silos with deduplication and golden record governance. - Built an integrated consent registry and DSAR management module. DSAR workflows include identity verification, data discovery across connected systems, redaction, approval checkpoints, and documented fulfillment—all timestamped for audit. - Integrated ERP with legacy payroll, MES, and finance systems via API gateway and ETL pipelines. Data quality rules enforced validation and minimization; retention automation purges stale records per policy, with legal hold capabilities. - Localization and governance: Country-specific legal bases, purpose codes, and privacy notices incorporated; configurable retention by data category; out-of-the-box RoPA and DPIA evidence reports for auditors.

Phase 4: Business Process Optimization - DSAR process: Introduced a unified intake portal, automated triage, and a RACI model with SLAs (acknowledge in 72 hours; fulfill within 30 days). Dashboards track throughput, cycle time, and backlog with executive reporting. - Vendor onboarding: Embedded DPA/SCC checks, DPIA triggers, and security questionnaires into procurement workflows. Exceptions require legal and security approvals within ERP. - Incident response: Defined severity tiers, communication playbooks, and regulator notification decision trees; ran tabletop exercises to validate readiness. - Governance: Established a Privacy Steering Committee chaired by the DPO to review metrics, DPIAs, and exceptions monthly.

Phase 5: Security Awareness Training - Delivered role-based training to 120 employees (HR, Customer Service, Procurement, IT). Modules covered data minimization, lawful bases, secure handling, phishing defense, and DSAR handling. - Conducted phishing simulations and knowledge assessments; updated onboarding training; created a network of “privacy champions” in each country operation.

1.5 Results & Impact

- Full compliance in four months: External counsel validated readiness; the regulator closed the warning without additional action.
- Financial risk avoided: Up to €2M in potential fines averted by timely remediation and demonstrable controls.
- Operational efficiency: Centralizing data and standardizing DSAR workflows saved 15 hours per week. Median DSAR fulfillment time fell from 14 days to 4 days; first acknowledgment consistently under 72 hours.
- Stronger security posture: 100% MFA coverage for privileged roles; zero critical vulnerabilities outstanding after monthly scans; comprehensive audit trails available for all access to personal data.
- Data quality and governance: Consolidated nine repositories into Origami ERP; duplicate personal records reduced by 42%; automated retention reduced over-retention of HR applicant data by 28% in the first purge cycle.
- Sustainable compliance: Complete RoPA, DPIAs for high-risk activities, standardized DPAs/SCCs, and dashboards provide ongoing visibility to leadership and auditors.
- Cultural uplift: 98% training completion; post-training assessments improved by 31 percentage points; phishing simulation click-through rates dropped from 18% to 3% over two campaigns.

Collectively, these outcomes turned a regulatory challenge into an opportunity to modernize operations, strengthen security, and build customer and employee trust.

1.6 Technologies & Services Used

- Services:
 - compliance-audit-gdpr
 - security-hardening
 - business-process-optimization
 - erp-implementation
 - security-awareness-training
- Technologies and capabilities:
 - Origami ERP (HR, Supplier Management, Customer & Order Management, Consent Registry, DSAR Management)
 - API gateway and ETL pipelines for system integration and data lineage
 - Data discovery and PII classification tooling; centralized RoPA/DPIA reporting
 - IAM with SSO (OIDC/SAML), MFA, RBAC, and quarterly access reviews

- Encryption at rest (AES-256) and in transit (TLS 1.2+); EU data residency; immutable backups
- Centralized logging/SIEM with immutable audit trails and alerting
- Endpoint detection and response; CIS-aligned hardening and vulnerability management
- Workflow automation for DSARs, vendor onboarding (DPA/SCC), retention, and legal holds

1.7 Conclusion

By combining a rigorous compliance-audit-gdpr with targeted security-hardening, a pragmatic erp-implementation of Origami ERP, disciplined business-process-optimization, and immersive security-awareness-training, we helped a pan-EU food processor move from regulatory exposure to demonstrable compliance and operational excellence in just four months. The program not only eliminated immediate enforcement risk and avoided significant fines, it also delivered durable value: faster customer and employee data responses, higher data quality, improved security, and clear governance. The client now operates with a defensible, auditable privacy posture—scalable across countries and adaptable to future regulatory changes—turning compliance into a competitive advantage.

About The Origami Corporation

The Origami Corporation is a leading technology consulting firm specializing in cloud migration, DevSecOps, cybersecurity, and digital transformation. We help organizations navigate complex technological challenges and achieve their business objectives through innovative, secure, and scalable solutions.

Connect With Us

Follow Us Online

LinkedIn: [The Origami Corporation](#)

Facebook: [@theorigamicorporation](#)

X (Twitter): [@OrigamiGlobal](#)

Telegram: [@theorigamicorporation](#)

Contact Information

Europe & Americas

- **Email:** office@theorigamicorporation.com
- **Phone:** +359 878 686 627

Asia-Pacific, Middle East & Africa (APMEA)

- **Email:** office.apmea@theorigamicorporation.com
- **Phone:** +41 77 924 2245

Ready to Get Started?

SCHEDULE A MEETING

Ready to transform your technology infrastructure? Contact us today to discuss how we can help your organization achieve similar results.