Bridging Privacy and AI Act Compliance

Mapping and Categorisation as a Shared Backbone

Mickaël Tome | Avocat à la cour

Data Privacy Day 2026

⚠ THE CHALLENGE

Navigating the Regulatory Crossroads

Many AI systems process personal data—both GDPR and AI Act apply simultaneously.

Organizations face parallel compliance tracks that duplicate compliance efforts, create inconsistent approaches, and miss critical synergies.

The Cost of Parallel Tracks

Financial Costs

Duplicate tools, assessments, and external advisors drain budgets unnecessarily.

Operational Costs

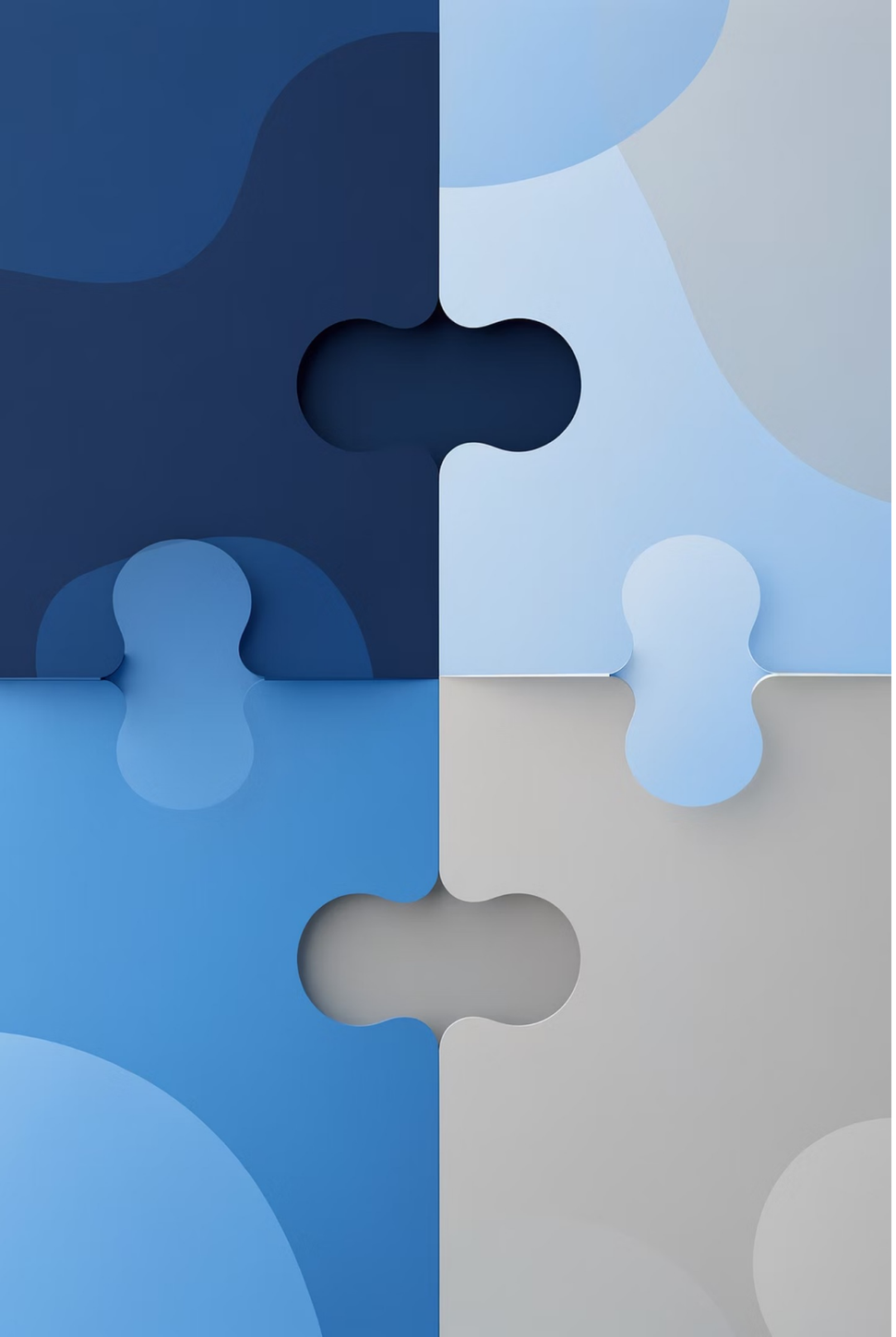
Redundant interviews, documentation, and reviews waste valuable time and resources.

Strategic Costs

Inconsistent risk assessments and missed integration opportunities weaken governance.

Every hour spent reinventing the wheel is an hour not spent on substantive compliance.

Organizations with mature GDPR compliance already possess some of the capabilities needed for AI Act compliance.



Build on What Exists

01

Unified Inventory

Single structure capturing data processing activities and AI systems for both frameworks.

02

Harmonized Risk Classification

Align GDPR's risk-based approach with AI Act's explicit tiers for consistent prioritization.

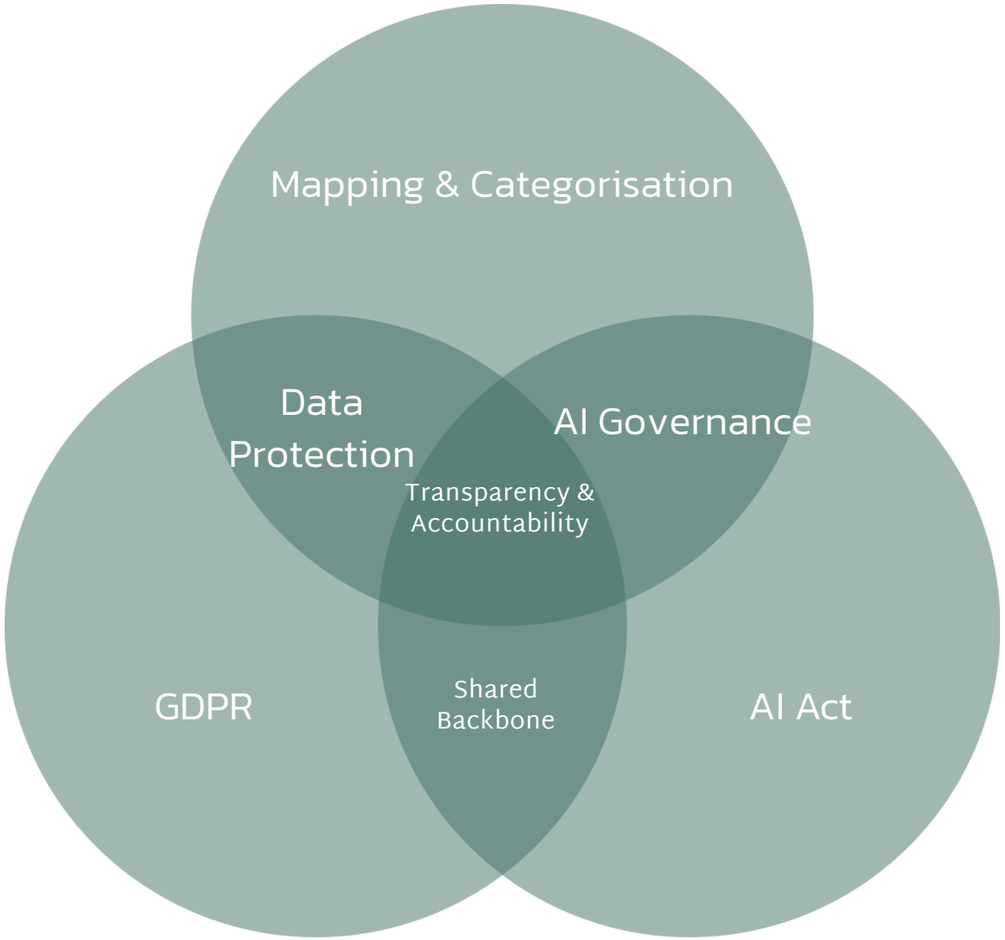
03

Faster Compliance

Achieve AI Act compliance more efficiently by leveraging existing GDPR foundations.

REGULATORY OVERLAP

The Natural Intersection



This overlap reflects shared European values of transparency, accountability, and protection of fundamental rights.

Key Integration Areas

- Records of processing activities and AI system documentation
- Risk-based approach & assessments
- Purpose limitation and intended use controls
- Transparency and disclosure obligations
- Human oversight and automated decision-making

Parallel Mapping Requirements

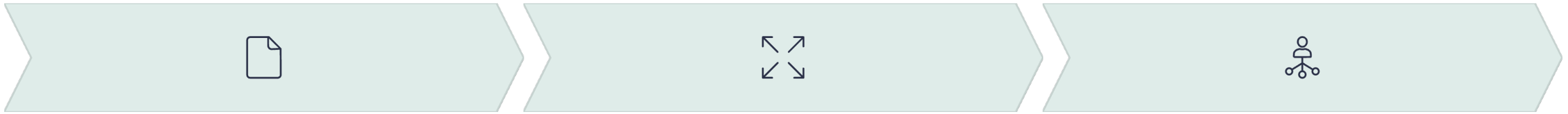
GDPR Requirement	AI Act Parallel	Integration Opportunity
Records of Processing Activities (Art. 30)	Technical documentation (Art. 11)	Unified inventory capturing both data flows and AI systems
High-risk processing requiring DPIA	AI risk categorization (prohibited, high-risk, limited, minimal)	Harmonized risk classification matrix
Purpose Limitation (Art. 5(1)(b))	Intended Purpose Documentation	Shared purpose definition and scope controls
Data Minimization (Art. 5(1)(c))	Data Governance for training data (Art. 10)	Integrated data governance framework
Automated Decision-Making (Art. 22)	Human Oversight Requirements (Art. 14)	Unified human-in-the-loop protocols

FOUNDATION

Mapping: a Key Compliance Foundation

You cannot comply with what you do not know you have. Mapping serves critical functions: visibility into data and AI systems, scoping regulatory requirements, enabling risk assessment, targeting controls, ensuring audit readiness, and tracking changes over time.

From Data Mapping to AI Mapping



Basic RoPA

Standard GDPR records of processing activities documenting data flows and purposes.

Extended Inventory

Add AI-specific fields to capture system classification, provider status, and conformity assessment.

Unified Backbone

Integrated view linking data processing, AI systems, assessments, and controls in one structure.

Essential Fields for Unified Inventory

Core Identification

- System/Process ID and name
- Business and technical owners
- AI system flag and provider/deployer status

Data Processing (GDPR)

- Purpose of processing (and lawful basis)
- Categories of data subjects and personal data
- Categories of recipients
- International transfers
- Retention period and security measures

AI System Fields (AI Act)

- AI risk classification (prohibited/high/limited/minimal)
- High-risk basis (Annex I or III reference)
- Intended purpose and deployment context
- Model type and training data description
- Conformity assessment and registration status
- Human oversight measures

Practical Implementation Approaches

Option A: Extend RoPA

Add AI-specific fields to existing records of processing activities. Fastest approach for mature privacy programs.

Option B: Linked Inventories

Maintain separate but cross-referenced inventories. Cleaner data model with explicit relationships.

Option C: Enterprise Platform

Implement comprehensive governance platform. Most robust solution with higher initial investment.

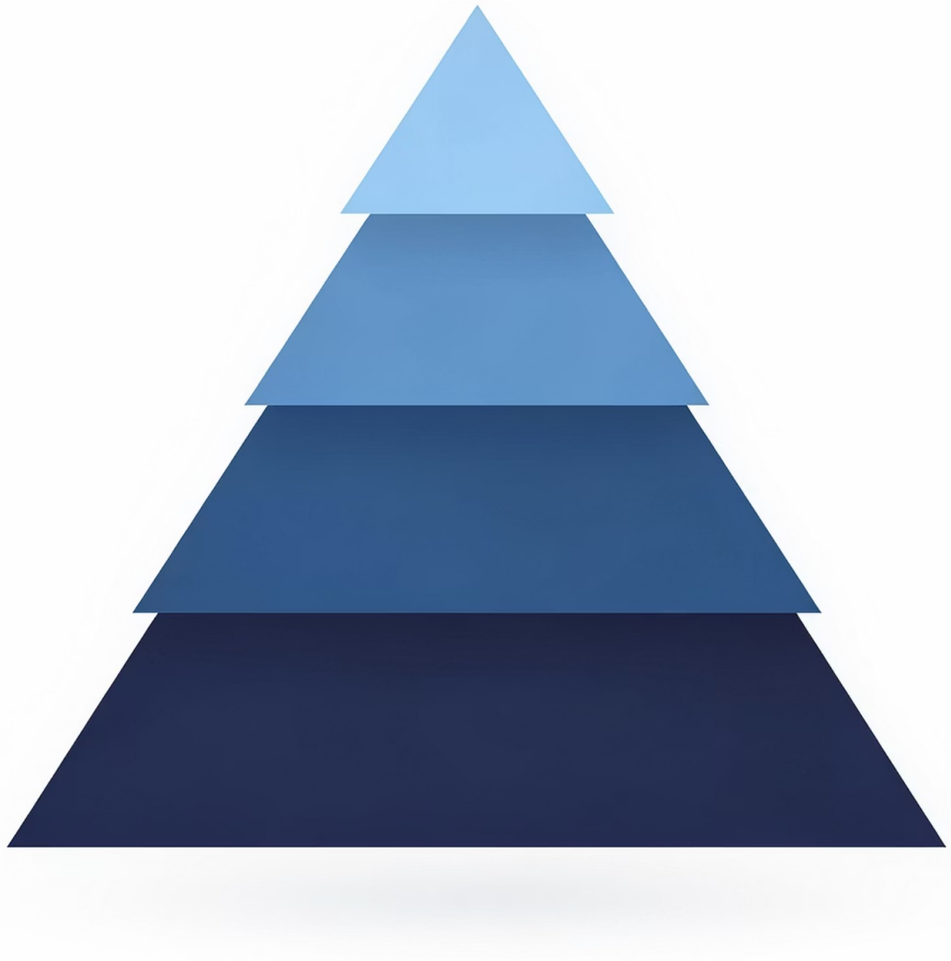
Do not Forget Shadow AI: Use procurement controls, network monitoring, and amnesty programs to surface hidden AI tools.

The Shadow AI Challenge

Many AI systems operate outside formal governance—purchased by business units, embedded in SaaS tools, or developed by individual teams. This "shadow AI" creates compliance blind spots.

Detection Strategies

- Procurement review and vendor questionnaires
- Network traffic analysis for AI API calls
- Employee surveys and amnesty programs
- Regular business unit audits



RISK-BASED

Categorisation: Risk-Based Regulation

Both GDPR and AI Act embrace risk-based approaches, calibrating obligations based on potential harm. Higher-risk activities face stricter requirements; lower-risk activities have lighter burdens. This shared philosophy enables unified risk categorisation.

GDPR Risk Assessment Framework

DPIA Triggers (Article 35)

Data Protection Impact Assessments required when processing is "likely to result in high risk to rights and freedoms":

- Systematic evaluation based on automated processing with legal/significant effects
- Large-scale processing of special category data (Art. 9) or criminal data (Art. 10)
- Systematic monitoring of publicly accessible areas at large scale

Supervisory Authority Positive List(s) & EDPB Criteria

National authorities identify high-risk processing:

- Biometric data
- Genetic data
- Systematic employee monitoring...

EDPB criteria (2+)

- Evaluation or scoring (incl. profiling
- Automated-decision making
- New technological solutions...

AI Act Risk Tiers

Prohibited

Social scoring, manipulative AI, certain biometric uses—DO NOT DEPLOY

High-Risk

Annex I (safety) + Annex III: HR, credit scoring, education, law enforcement, healthcare

Limited Risk

Chatbots, deepfakes—transparency obligations apply

Minimal Risk

All other AI systems—no mandatory requirements

Unified Risk Classification Matrix

	AI Act: Minimal/Limited	AI Act: High-Risk	AI Act: Prohibited
GDPR: Standard Processing	Minimal/Standard Routine Compliance	High AI Risk/Standard Privacy AI-Focused Compliance	DO NOT DEPLOY
GDPR: High Risk (DPIA Required)	Standard AI Risk/High Privacy Privacy-Focused Compliance	High Risk in Both Maximum Compliance	DO NOT DEPLOY

This matrix enables consistent prioritization, efficient resource allocation, and clear risk communication to stakeholders.

High-Risk Intersections (under both frameworks)

HR & Recruitment AI

High-risk under Annex III + DPIA required for profiling affecting employment decisions.

Credit Scoring AI

High-risk under Annex III + DPIA required for significant financial effects on individuals.

Biometric Systems

High-risk classification + special category data processing under Article 9 GDPR.

Healthcare AI

Often Annex I (medical device) + health data processing under Article 9 GDPR.

These use cases require integrated DPIA/FRIA, comprehensive documentation, robust human oversight, conformity assessment, and EU database registration.

GOVERNANCE

Potential Organizational Models for Integration

Integrated Model

Structure: AI governance within expanded privacy function

Best for: Moderate AI use, strong existing privacy team

Advantage: Unified accountability and streamlined processes

Federated Model

Structure: Separate teams with shared tools and processes

Best for: Larger organizations with significant AI deployment

Advantage: Specialized expertise while maintaining coordination

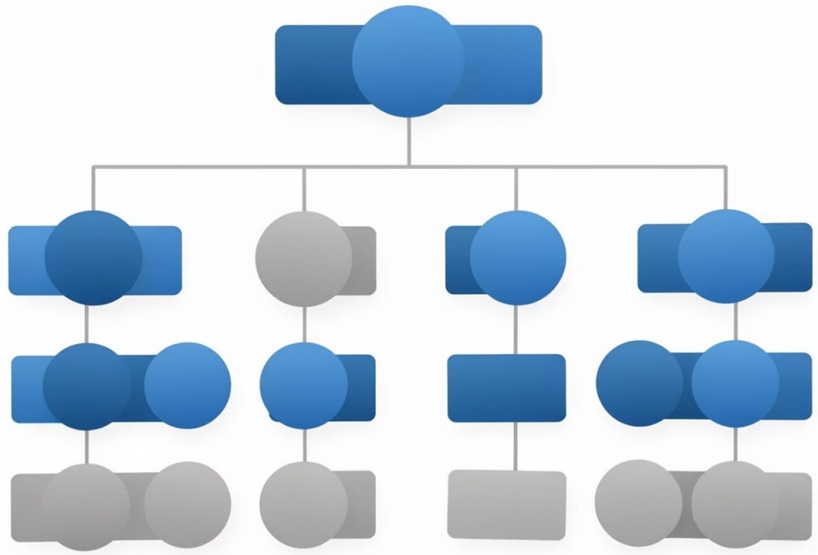
Centre of Excellence

Structure: Cross-functional team sets standards

Best for: Distributed AI development, matrix organizations

Advantage: Consistent standards across diverse business units

Key Roles and Responsibilities



The Evolving DPO Role

Data Protection Officers naturally extend into AI governance through existing responsibilities: DPIAs for AI processing, Article 22 automated decision-making, data quality requirements, and security of AI systems.

AI Officer/Responsible AI Lead

Dedicated AI governance roles require clear delineation from DPO responsibilities and strong coordination mechanisms to avoid gaps or conflicts.

Business Unit Accountability

Business units deploying AI systems retain ultimate accountability for compliance regardless of central governance structure.

Shared Processes Across Models

Joint DPIA/FRIA Assessments

One integrated process achieving dual compliance instead of separate assessments.

Unified Vendor Due Diligence

Combined privacy and AI questionnaires streamline third-party risk assessment.

Integrated Training Programs

Cross-functional awareness building for both privacy and AI governance teams.

Common Tooling and Workflows

Single inventory platform with shared workflows reduces duplication and inconsistency.

Key principle: Separate teams can succeed with a shared backbone of tools, processes, and data.

IMPLEMENTATION

Implementation Roadmap

Phase 1: Discovery

Assess current RoPA, conduct AI census, identify shadow AI, populate unified inventory

1

Phase 2: Classification

Apply dual classification, map to risk matrix, prioritize high-risk systems (high-risk in both frameworks)

2

Phase 3: Documentation

Conduct combined assessments, implement controls, complete registrations

3

Phase 4: Governance

Lifecycle management, monitoring, audit, continuous improvement

4

Start with high-risk systems (both)—highest risk, clearest ROI from integrated approach.

⚠ CHALLENGES

Key Challenges and Mitigations

Definitional Mismatches

Challenge: Terms differ between frameworks

Mitigation: Create internal glossary; track applicability separately

Different Maturity Levels

Challenge: GDPR mature, AI Act emerging

Mitigation: Leverage GDPR foundation but don't assume sufficiency

Organizational Resistance

Challenge: Teams protective of territory

Mitigation: Build business case; demonstrate quick wins; secure executive sponsorship

Technology Gaps

Challenge: Existing tools may not support integration

Mitigation: Cross-training; hire T-shaped skills; use external expertise

Over-Simplification Risk

Challenge: Losing clarity on requirement sources

Mitigation: Maintain clarity on which requirement comes from which regulation

Regulatory Uncertainty

Challenge: AI Act guidance still evolving

Mitigation: Build flexible frameworks; monitor guidance; document assumptions

Critical Pitfalls to Avoid

Assuming GDPR Compliance = AI Act Compliance

The overlap is significant but not complete. AI Act introduces new requirements beyond GDPR scope.

Ignoring Cultural Resistance

Integration requires change management. Address team concerns and demonstrate value early.

Over-Simplifying the Integration

Maintain nuance about which requirements come from which regulation to ensure complete compliance.

Underestimating Resource Needs

Integration saves resources long-term but requires upfront investment in tools, training, and process redesign.

Efficiency Gains: Parallel vs. Integrated

Activity	Parallel Approach	Integrated Approach
Inventorying systems and data	Two separate inventories	One unified inventory
Impact assessments	DPIA + FRIA separately	Combined assessment
Vendor due diligence	Two review processes	Single unified review
Stakeholder interviews	Interviewed twice	Single engagement
Tooling and platform costs	Multiple platforms	Consolidated platform

Strategic Benefits Beyond Compliance

Holistic Risk Visibility

Single unified view across privacy and AI domains enables better decision-making and resource allocation.

Faster AI Deployment

Streamlined compliance clearance accelerates time-to-market for AI initiatives while maintaining governance.

Stronger Regulatory Position

Demonstrates mature, integrated governance to supervisory authorities and builds credibility.

Enhanced Stakeholder Trust

Coherent story on responsible AI and privacy strengthens customer, employee, and partner confidence.

Key Takeaways

Don't Reinvent the Wheel

Build AI Act compliance on your existing GDPR foundation. Organizations with mature privacy programs already have some of the needed capabilities.

Mapping + Categorisation = Shared Backbone

Unified inventory and integrated risk matrix create efficiency, consistency, and comprehensive governance.

Start Now

Extend your inventory, classify your AI systems, align your teams. Proactive integration beats reactive scrambling.

> "The question is not whether privacy and AI governance will converge. The question is whether your organization will lead this convergence proactively or be forced into it reactively."

Thank you for your attention !

Mickaël Tome | Avocat à la cour

mickael@togouna-tome.eu

(+352) 661 180 559