DPOBOARD PERSPECTIVES · WHITE PAPER

AI Governance in the Enterprise: Building a Defensible Framework Across Every Function

How multinational organizations are turning fragmented privacy and AI regulation into one coordinated, function-aware governance program.

DPOBOARD, LLC

August 2026

EXECUTIVE SUMMARY

Privacy, data protection, and AI governance have become one conversation — most organizations are still running three.

Multinational enterprises now sit at the intersection of long-standing privacy law, fast-evolving AI-specific regulation, and internal functions — HR, Marketing, IT, Legal, Engineering, Procurement, Communications, and more — that each create and consume risk differently. Treating these as separate compliance tracks is the single most common reason governance programs stall.

This paper outlines a practical framework for unifying privacy, data protection, and AI governance into a single operating model — one built to scale across departments, jurisdictions, and the shifting regulatory timeline described in Section 2.

3

regimes now routinely apply to a single enterprise AI use case — privacy law, sector rules, and AI-specific regulation

8+

distinct business functions typically deploy or touch AI systems in a multinational organization

1

governance model needed — not one per function, one per jurisdiction, or one per system

> ***"The organizations managing this well aren't the ones with the most policies. They're the ones whose policies actually match how each function uses data and AI."***

KEY TAKEAWAYS

- AI-specific obligations are arriving on a staggered timeline layered on top of existing privacy law — programs need to track both, not sequence them.
- Risk is not evenly distributed across departments; a one-size-fits-all training or policy set under-serves high-exposure functions and over-burdens low-exposure ones.
- A durable program separates what is permanent (governance structure, roles, escalation paths) from what changes often (jurisdiction-specific obligations, system inventories).

A REGULATORY LANDSCAPE IN MOTION

01

Three layers of obligation, moving at three different speeds.

General privacy law forms the baseline: the EU's GDPR and the UK GDPR, the CCPA as amended by the CPRA in the United States, and a growing list of comparable state and international regimes. These frameworks are now mature, with well-established enforcement patterns and, for most multinational organizations, existing compliance programs.

AI-specific regulation is newer and still moving. The EU AI Act (Regulation 2024/1689) entered into force in August 2024 on a phased timeline: general provisions and prohibited-practice rules took effect in February 2025, and general-purpose AI model obligations followed in August 2025. The Act's most operationally demanding tier — obligations for high-risk AI systems under Annex III — was originally set to apply from August 2, 2026. Following the EU's Digital Omnibus on AI, which entered into force in July 2026, that deadline has been deferred: Annex III high-risk obligations now apply from December 2, 2027, and Annex I product-embedded high-risk systems from August 2, 2028.

The practical implication is not that the pressure is off — it is that the runway just got longer for organizations that use it. Enterprises that treat the deferral as a reason to pause risk having to compress eighteen months of governance work into a few final weeks, as many did in the run-up to GDPR.

Layered on both is a third dimension: sector and function-specific rules — employment law touching HR's use of algorithmic tools, sectoral guidance affecting health and safety data, marketing-specific consent and profiling rules, and procurement obligations that increasingly flow down AI-vendor risk to the enterprises that engage them.

> ***“A deferred deadline is a planning asset, not a reason to stand down.”***

WHY FUNCTION MATTERS

02

The same regulation lands differently in every department.

A single privacy or AI governance policy, delivered identically to every employee, tends to under-inform the functions carrying the most exposure while over-informing those carrying the least. Mapping exposure by function is what makes a governance program — and the training that supports it — actually meaningful.

FUNCTION	ILLUSTRATIVE EXPOSURE	TYPICALLY ENGAGED REGIMES
Human Resources	Algorithmic hiring tools, employee monitoring, workforce analytics	Privacy law, AI Act (employment-context systems), labor law
Marketing	Profiling, targeted advertising, consent management	Privacy law, ePrivacy/cookie rules, consumer protection
IT	Infrastructure access controls, vendor AI tooling, data residency	Privacy law, sector security rules, AI Act (deployer duties)
Legal	Contract risk, vendor terms, regulatory response	All applicable regimes
Engineering	AI/ML system design, model risk, data pipeline governance	AI Act (provider duties), privacy-by-design obligations
Procurement	Third-party AI and data-processing vendor risk	Privacy law (processor terms), AI Act (supply chain)
Communications	Public disclosures, incident communications	Privacy law (breach notice), securities disclosure where applicable
EHS	Health and safety monitoring data, wearable/sensor data	Privacy law, health-data-specific rules

Table is illustrative and not exhaustive; applicable regimes vary by jurisdiction and specific use case.

One model, three pillars, applied consistently across every function and jurisdiction.

Privacy by Design

Embedding privacy requirements into systems and processes at design time, not as a retrofit after launch.

Data Protection Controls

Technical and organizational measures — access control, encryption, vendor management — sized to actual data sensitivity.

AI Governance Oversight

Inventory, risk classification, and human oversight for AI systems across their lifecycle, mapped to applicable regulation.

The three pillars share a common backbone: a function-aware risk map, a single source of truth for obligations by jurisdiction, and role-based policy and training that reflects what each department actually does — rather than a generic, one-size-fits-all program.

A PRACTICAL ROADMAP

04

Five steps to move from fragmented compliance to coordinated governance.

01 **Build a cross-functional inventory**

Identify where AI systems and sensitive data actually live across departments — not just what IT knows about, but what Marketing, HR, and Engineering have adopted independently.

02 **Map obligations by function and jurisdiction**

Translate the regulatory landscape in Section 1 into a matrix of which rules actually apply to which team, in which country.

03 **Deliver role-based policy and training**

Replace generic, all-employee-only training with a base module for every employee plus targeted modules scoped to each function's actual risk.

04 **Implement an ongoing assessment cadence**

Move from a point-in-time audit to a recurring rhythm of risk assessment tied to new system launches and regulatory milestones.

05 **Sustain through governance, not heroics**

Establish a standing governance committee with clear ownership, so the program survives beyond the people who built it.

CONCLUSION

The advantage goes to organizations that unify now, on their own timeline.

Regulatory deadlines will keep shifting — that is the nature of a still-maturing area of law. What doesn't need to wait is the internal work: knowing where AI and sensitive data live, understanding which functions carry the most exposure, and building policy and training that reflects that reality. Organizations that do this work on their own schedule, rather than in reaction to the next enforcement deadline, consistently spend less and move faster when the rules do change.

ABOUT DPOBOARD

DPOBOARD helps multinational, multi-department organizations manage privacy, data protection, and AI governance risk as one coordinated program — including function-scoped training, risk assessments, and governance program design built around how each business actually operates.

Let's build a governance program that matches how your organization actually works.

DPOBOARD, LLC

1699 Wall Street, Mount Prospect, IL 60056

info@dpoboard.com · dpoboard.com

This white paper is provided for general informational purposes only and does not constitute legal advice. Regulatory timelines referenced herein, including EU AI Act deadlines, reflect publicly available information as of August 2026 and are subject to change. © 2026 DPOBOARD, LLC. All rights reserved.