MACMA
The Media, Audience & Content Marketing Association

omeda

AI Governance Checklist

This framework outlines essential domains of privacy and AI maturity, with a focus on turning regulatory requirements into strategic business value.

1. Governance & High-Level Framework Components

- □ Our organization uses a formal, documented privacy framework aligned to NIST, ISO, or AICPA (whichever is applicable to your organization)
- □ Policies address data lifecycle & classification, cross-functional ownership, and third-party risk
- □ Leadership views privacy as a long-term trust and innovation enabler—not just a compliance function or cost center
- □ A Privacy Steering Committee or governance board meets quarterly to evaluate risk and opportunity
- □ AI use and tools are integrated into overall data governance and reviewed regularly
- □ Risk Assessments are in place for all data repositories, based on data sensitivity retained

2. Data Minimization & Retention

- □ We only collect data necessary for defined business or audience purposes
- □ Retention policies are in place and enforced for every system and dataset
- □ Data minimization is actively discussed in product development and marketing campaign planning
- □ We regularly review what data we *don't need* and what it could expose if breached

3. Data Subject Requests (DSRs)

- □ We support data access, correction, deletion, and portability across all users—not just EU/UK
- □ Our systems can fulfill DSRs within regulatory timeframes (typically 30–45 days)
- □ Audience-facing tools allow users to manage their data and consent with minimal friction
- □ Teams understand that DSRs represent a broader shift toward user empowerment—not just a GDPR checkbox

4. Product Innovation & AI Use Cases

- □ Product teams understand and apply privacy-by-design (PbD) in their product lifecycle
- □ Static or behavioral data is used to inform product development responsibly
- □ We track which data contributes most to product innovation (vs. what's collected by default)
- □ AI models and content engines are tested against company values and output goals
- □ AI tools are risk-assessed to protect proprietary data, and users are trained on the safe and ethical use
- □ Teams review how AI-generated insights or recommendations might shift editorial tone or decision-making

5. Brand Trust, Consent, and Volume Reliance

- □ Privacy notices and AI disclosures are written clearly for each audience segment
- □ Consent is tracked and managed with transparency across every platform
- □ Audience retention is tied to trust and clarity—not just funnel size
- □ Sales is trained on best practices on how to effectively sell engagement and recency instead of volume

6. Bringing It Back to the Framework

This isn't just a checklist—it's a leadership tool.

☑ Privacy strengthens our brand reputation
☑ It unlocks ethical, sustainable innovation
☑ It enables cross-team alignment and audience transparency at scale

**Note: These are suggestions and not legal advice. Please consult with your legal counsel.*

Have questions? Feel free to connect!

Bettina Lippisch, VP, Privacy & Data Governance, CIPM | Omeda
www.linkedin.com/in/bettinalindner

Amanda Landsaw, CMO, CIPM | Endeavor Business Media
www.linkedin.com/in/amandalandsaw