O'Melveny

2026 Data Security & Privacy Compliance Check-In: Key Action Items for Organizations

As data security and privacy obligations continue to expand—driven by newly effective state laws, heightened risk assessment, and audit requirements, AI-specific regulations, updates to children's privacy rules, and evolving international data protection regimes—organizations should take proactive steps to evaluate and strengthen their compliance programs. The following checklist highlights priority action items drawn from significant US and international developments taking effect in or around 2026.

- [ ] Update privacy notices on an annual cadence and upon material change.
  - [ ] Ensure coverage of newly effective state laws, enhanced transparency on sensitive data, opt-out signals, and automated decision-making; align public-facing disclosures with actual processing to avoid enforcement risk.
- [ ] Maintain a current enterprise data and AI/ADMT inventory.
  - [ ] Map personal data flows, identify AI/ADMT use cases, classify risk levels, and document data uses to support disclosures, assessments, and audits under US state laws and the EU AI Act timelines.
- [ ] Implement and regularly test privacy preference selection opt-outs (including universal signals).
  - [ ] Validate end-to-end functionality of GPC/opt-out preference signals with visible confirmation, ensure cookie banner symmetry/consent, and test performance across channels and load.
- [ ] Prepare for independent cybersecurity audits where applicable.
  - [ ] Track thresholds and phase-ins, with first certifications due April 1 in 2028–2030 depending on size.
- [ ] Strengthen third-party/vendor management.
  - [ ] Update DPAs and diligence to reflect state-specific transparency and profiling/ADMT obligations (e.g., Minnesota's right to a list of specific third parties actually receiving data; Colorado processor disclosures for biometrics); verify vendor-operated rights mechanisms function as described.
- [ ] Create entity-specific procedures for applicable risk assessments.
  - [ ] Cover high-risk processing (selling/sharing PI, sensitive PI, significant-impact ADMT/profiling, training ADMT/biometrics) and track jurisdictional deadlines.