



Privacy Priorities in 2024

- Assess applicability of new state laws and determine compliance requirements.
- Update public-facing privacy notice(s) if required.
- Refine/Update/Automate data subject request processes.
- Accurately disclose selling/sharing of data with third parties and provide opt-in/out as required.
- Update/develop data processing agreements if required.
- Review processing of children's data, health data, and other sensitive information; ensure appropriate consent is obtained.
- Implement/refine/continue PIA/DPIA process.
- Refresh internal data protection policies and procedures (e.g., employee privacy notice, data subject request training, data classification policies).
- Ensure data mapping is up to date (including tracking technologies).
- Build and regularly update incident response plans and conduct tabletop exercises to practice implementing them.
- Develop role-based privacy trainings and materials.
- Address applicable data transfer requirements (e.g., the EU-U.S. Data Privacy Framework).
- Incorporate privacy into AI governance (e.g., AI risk assessments, internal AI policy, strategic risk mitigation measures and functionality if offering AI products/features, monitoring AI legislation).
- Effectively communicate privacy-legal risk and value-add of a data privacy program to business stakeholders.