Insights, News & Events

7 THEMES DRIVING DATA PRIVACY IN 2026: WHAT TECH COMPANIES NEED TO KNOW

Insights
Mar 25, 2026

7 Themes Driving Data Privacy in 2026: What Tech Companies Need to Know

As AI use accelerates, regulators are focusing more on data privacy enforcement – which means businesses need to make compliance a strategic priority. For tech companies in particular, the volume and sensitivity of data flowing through their systems creates heightened exposure under an expanding patchwork of data privacy laws. Whether you are a startup scaling quickly, or an established technology company integrating AI tools into your operations, here are seven things you need to know and seven steps you should consider taking now.

1. Evolving Privacy Laws Are Changing Employer Obligations

Tech companies often assume privacy regulations primarily apply to consumer-facing giants. In reality, many laws are triggered based on revenue thresholds, personal data volume, or the location of the individuals whose personal data you process.

Tech companies may be subject to:

- The EU's General Data Protection Regulation (GDPR)
- The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA)

Related People

Logan S. Booth, CIPP/US
Of Counsel

720.644.2889

Brett P. Owens
Partner

813.769.7512

- Other comprehensive state privacy laws (like in Colorado, Virginia, and Texas)
- Industry-specific rules (HIPAA, GLBA, COPPA)
- International frameworks such as Canada's PIPEDA and Brazil's LGPD

Laws may cover existing and prospective employees' data in addition to customer information. Be sure to know what rules apply to your organization.

2. Employee Data Is a Growing Risk Area

Tech companies collect and process substantial amounts of workforce data, including:

- Applicant materials and background checks
- Payroll and tax records
- Health and benefits information
- Internal communications
- Device monitoring and productivity analytics
- Access logs and system activity

Several state and international privacy frameworks now give employees the right to access, correct, or delete certain personal data. Employers must ensure HR systems, monitoring tools, and SaaS platforms align with applicable notice, disclosure, and opt-out requirements. Remote work and distributed teams increase confusion on which jurisdictional rules apply.

Remember that data cannot be compromised if it's not collected or has been properly disposed of before a breach occurs. To that end, best practices include:

- Collecting only data necessary for a defined business purpose
- Establishing written data retention schedules
- Implementing automated deletion protocols
- Regularly auditing legacy systems and archived records

Daniel Pepper, CIPP/US

Partner

303.218.3661

Service Focus

AI, Data, and Analytics

Privacy and Cyber

Industry Focus

Tech

Resource Hubs

AI Governance Hub

3. Security Alone Is Not Enough

Data security and data privacy are related but distinct. Security protects data from unauthorized access, while privacy governs how data is lawfully collected, used, shared, and retained. Complying with data security and privacy rules requires both technical safeguards and governance controls.

You may have strong security controls, yet still face liability if your business:

- Uses employee or customer data for undisclosed purposes
- Lacks a lawful basis for processing data
- Fails to provide required privacy notices
- Shares or sells data with third parties without requisite consent

4. Third-Party Risk Is Employer Risk

Tech companies rely heavily on third-party providers, including cloud hosting services, payroll and HR platforms, analytics vendors, AI tools, CRM and marketing platforms, and messaging platforms.

Most privacy laws hold businesses responsible for how vendors and other third parties handle the personal data they receive.

Employers should conduct thorough vendor due diligence, including:

- Reviewing and negotiating Data Processing Agreements (DPAs)
- Confirming vendors maintain adequate and documented security controls
- Understanding sub-processors and cross-border transfers
- Limiting vendor access to necessary data only
- Ensuring data disposal requirements are met once the engagement ends

5. AI Amplifies Privacy Exposure

The rapid adoption of generative AI tools introduced additional legal complexity for tech companies. Risk areas include employees uploading confidential or personal data into public AI tools, training models on scraped data without consent, inadvertent disclosure of personal information in AI outputs, and lack of transparency around automated decision-making.

To mitigate these risks, your business should adopt written AI usage policies, delineate clear internal guardrails, implement workforce training, and review the AI terms and use for vendors and other third-party affiliates.

6. Breach Response Preparedness Is Essential

All US states and many international jurisdictions have breach notification laws, which impose notification obligations for compromises to personal data, sometimes within tight timeframes (for example, 72 hours under GDPR). Failure to respond promptly and appropriately can significantly increase legal liability and regulatory penalties.

You can prepare by creating a written incident response plan, establishing escalation procedures, working with privacy counsel, and testing communications protocols.

7. Privacy and Security Maturity Is Now a Competitive Expectation

Enterprise customers and investors increasingly conduct privacy and security due diligence before engaging technology vendors. Weak governance can delay or derail opportunities with customers and investors.

These parties look for clear and accessible privacy notices, documented data governance practices, regular risk assessments that track enterprise maturation, and continuous oversight.

Practical Steps for Tech Companies

To reduce risk and strengthen compliance, you should consider:

1. Conducting data mapping exercises to understand what personal data your business collects and where it resides.

2. Reviewing employee and applicant privacy notices for compliance with applicable laws.
3. Auditing vendor agreements for appropriate data protection provisions.
4. Implementing or updating AI governance policies.
5. Pressure testing your cybersecurity policies and procedures for efficacy and comprehensiveness.
6. Establishing or refreshing an incident response plan.
7. Evaluating data retention and deletion practices.

Conclusion

Make sure you are subscribed to Fisher Phillips' Insight System to receive the latest content relevant to your tech business. If you have questions, contact the authors of this Insight, your Fisher Phillips attorney, or any attorney on our Tech Industry Team or Privacy and Cyber Team.