

A red horizontal banner with the text 'Technology Industry Spotlight' in white, sans-serif font. The banner is positioned over the lower part of the background image, which shows a person in a blue shirt interacting with a futuristic digital interface.The main title of the report is displayed in large, bold, white, sans-serif font. It is positioned in the lower left quadrant of the image, overlapping the background image of a person and the digital interface. The text is arranged in four lines: 'Global Privacy, AI,', 'and Data Governance', 'for Resilience and Trust'. The background image shows a person in a blue shirt interacting with a futuristic digital interface that includes a login form with fields for 'username' and a password (represented by asterisks), an 'OK' button, and various icons representing different aspects of technology and security, such as a padlock, a globe, a dollar sign, a document, a building, a mail envelope, and a bell.

Privacy and Data Governance for the Tech Industry

The technology industry is constantly innovating. Whether it's software, hardware, or something that blends the two, tech companies always have an eye on the horizon for what comes next. To fuel that ambition, companies need accurate, reliable data so they can draw insights that enable strategic decision-making and better serve their customers. But technology companies must also be aware of evolving data privacy laws and regulations across the globe, and how the data they collect is subject to compliance obligations.





Understanding Exposure

Companies will experience different levels of exposure to privacy laws depending on the nature of the data they collect and where they operate. For instance, when comparing B2B and B2C companies, B2C businesses tend to collect more customer data. Since privacy laws are more focused on individuals' personal data, B2C companies are more likely to face compliance obligations. Additionally, those companies must understand the various jurisdictions whose privacy laws they must comply with.

With more than 20 states enacting their own privacy laws and international regulations such as the EU's General Data Protection Regulation (GDPR) now in effect, it's imperative for technology companies to stay on top of the evolving regulatory landscape.



Privacy vs. Security

Privacy and security are related, but they aren't the same. Security incidents include matters of confidentiality, integrity, or system data. Privacy incidents, on the other hand, specifically relate to unauthorized access of personal information or its use, loss, mishandling, and disclosure. While safeguarding all data is critically important for businesses, it's important to understand whether an issue is security or privacy related since the affected stakeholders and responses will vary.



Third-Party Compliance and Tracking

Outsourcing a function or using third parties for specific tasks does not shift risk to those vendors. Technology companies often rely on cloud providers, data processors, implementation partners, analytics tools, marketing platforms, AI vendors, and other service providers that may collect, process, store, or access personal information. Organizations remain responsible for understanding those data flows, contract obligations, and compliance risks, even when the underlying activity is performed by a vendor.

Companies must also be aware of how they're using tracking technology on company websites, digital platforms, and applications. This includes browsing cookies, software development kits, pixels, session-replay tools, and similar technologies. When a user visits a website or uses a digital product, the company should provide appropriate notice and choice mechanisms so users can understand and manage applicable tracking preferences. Enforcement risk often arises when companies fail to configure, present, or honor these mechanisms correctly.

Organizations should be aware that the more complicated and numerous their tracking technology is, the more work will be required to maintain compliance. Tracking tools deployed across websites, mobile applications, product dashboards, customer portals, embedded content, and third-party integrations must all be configured appropriately. Because most of these are public-facing assets, regulators can easily audit and verify if companies are complying with privacy laws and requirements as intended.



Data Collection

Technology companies need to be aware of what data they're collecting and ensure that they have a purpose behind its collection. Data breaches remain a prominent cyberthreat, with the exfiltration of sensitive company and personal data a particularly valuable asset. By gathering data that is not needed for a defined business reason, companies increase the risk of exacerbating the damage a breach or misuse can cause.

Organizations must also be intentional with their data collection and governance, bearing in mind the purpose they're going to use the data for. They must understand what data they collect, where they are storing it, how long they are required to store it for, and how they handle it over that duration.

Technology companies must also be aware of the implications AI presents. As AI features move quickly from experimentation to production, organizations should build privacy reviews into product development, release, and change-management processes before launch.

Effective data governance practices can help technology companies fuel innovation while remaining compliant with regulations in the jurisdictions where they operate. It can also help them increase resilience against the ongoing challenge of cyberthreats and inappropriate use of personal data while building trust among their customers and stakeholders.





Build Trust Through Stronger Privacy, AI, and Data Governance

BDO's [Global Privacy, AI, and Data Governance for Resilience and Trust](#) e-book looks at how leaders can build operational, trackable governance frameworks that support innovation while reducing regulatory, reputational, and business risk.

BDO's [Privacy & Data Protection Services](#) help organizations develop and implement a comprehensive privacy and data protection strategy to maintain global compliance and responsibly handle personal information.

Explore the **Global Privacy, AI, and Data Governance for Resilience and Trust** e-book ►



Have questions or want to learn more? Contact us!

At BDO, our purpose is to be the people you count on to grow with confidence and achieve what matters most. Our professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization. We are proud to be an ESOP company, inspiring an ownership mindset that enables our collective success.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.

© 2026 BDO USA, P.C. All rights reserved.

