



The 5 Things Every Business Needs to Know About the Modern Consumer Privacy Landscape

Insights

11.13.24

It's no longer good enough for your business to have a reactive approach to consumer privacy – you need a proactive strategy to manage compliance, foster consumer trust, and stay competitive in this modern era. While many businesses might think they have a handle on their privacy obligations, there are five key essentials that often go overlooked. Fisher Phillips has unveiled its [new FP U.S. Privacy Hub](#) to help businesses navigate these five realities and other common situations that catch unsuspecting businesses unaware.

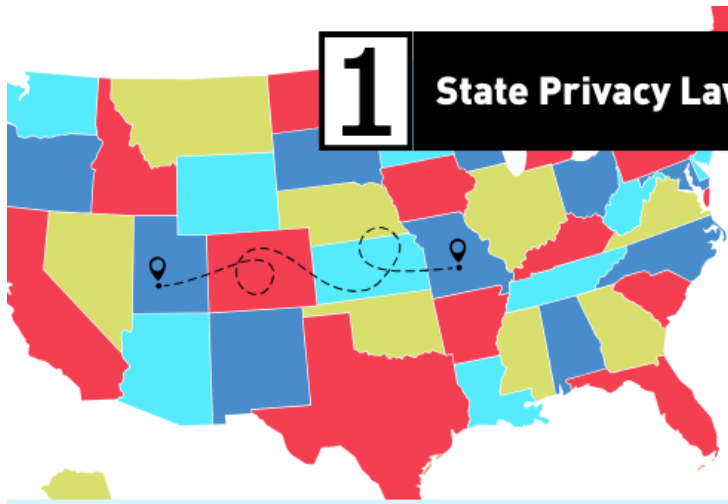
1. State Privacy Laws Can Reach Across State Borders

It often surprises businesses to learn state privacy laws often apply beyond state borders, triggered by the collection of personal data from residents of those states, including through a website. That means that compliance isn't just for in-state entities. Any business meeting certain thresholds – such as specific revenue levels or the number of residents whose data is collected – must comply with state laws, even if they don't have a physical presence in the state.

You can find a comprehensive listing of state privacy laws to help you identify potentially applicable laws on [the FP U.S. Privacy Hub here](#).


Some prime examples include California's Consumer Privacy Rights Act (CPRA) and Virginia's Consumer Data Protection Act (CDPA). They both impose strict compliance requirements that extend to companies meeting certain thresholds, like handling data on a specified number of state residents or surpassing minimum revenue levels.

Failing to meet the compliance obligations for these state laws can expose your business to regulatory actions and fines, which makes it critical to understand the specific applicability thresholds of each state where consumer data is collected.



1 State Privacy Laws Can Reach Across State Borders

Any business meeting certain thresholds – such as specific revenue levels or the number of residents affected – must comply with state laws, even if they don't have a physical presence in the state.



2. Consumers Now Have Broad Privacy Rights: Access, Deletion, and Beyond

Consumer data rights are at the core of most privacy laws. These rights – commonly including access, deletion, correction, and opt-out options – affect how businesses must manage and respond to data subject requests.

You can find a state-by-state review of your obligations when responding to consumer requests on [the FP U.S. Privacy Hub here](#).

But compliance requires more than acknowledgment. Your business needs to build an infrastructure to manage these data subject requests efficiently and securely. You'll also need to establish or update internal processes for handling access and deletion requests, ensuring that each request is verified (where verification is required or permitted by the law), fulfilled within mandated timeframes, and documented for compliance purposes.

2 Consumers Now Have Broad Privacy Rights

ACCESS	DELETION	CORRECTION	OPT-OUT
			

Your business needs to build an infrastructure to manage these rights requests efficiently and securely.



3. Your Business Has Data Collection and Transparency Obligations

Many state laws require businesses to disclose how they collect, use, and share personal data in privacy notices and website disclosures. That means you need to have clear and comprehensive privacy policies – and need to stay up to speed to ensure you make regular updates as the law evolves.

If you haven't yet developed a privacy policy, this is a must-do on your compliance checklist. But even if you have a policy, you must regularly review and update it to reflect the ever-changing landscape when it comes to data handling practices or regulatory standards. For example, as new state laws take effect, your privacy notices may need to address additional requirements such as data processing purposes or retention periods. Some state laws, including the CCPA, require an annual update to existing privacy policies as well. A proactive approach to policy updates not only protects against compliance issues but also signals to consumers that you take data privacy seriously.

The attorneys behind the FP U.S. Privacy Hub can assist your business in creating or updating your privacy policy. [You can find a full menu of our services here.](#)



3 Your Business Has Data Collection & Transparency Obligations

You need to have clear and comprehensive privacy policies. This is a must-do on your compliance checklist.



4. You Need to Manage Your Vendors and Third-Party Data Sharing Services

If one of your vendors violates a privacy obligation, causes a data breach, or otherwise fails to live up to expectations, you can't just point the finger at them and hope they'll accept all responsibility. Because your privacy obligations don't stop at your organization's walls, you need robust vendor agreements and monitoring systems to ensure third-party data processors comply with their compliance obligations.

- To manage third-party compliance and ensure robust vendor oversight, you first need to deploy a clear Data Processing Agreement (DPA) that outlines each party's responsibilities.
- You next need to conduct regular due diligence on vendor security practices, which includes performing scheduled audits.

- Overall, you should develop strong vendor relationships built on transparency and accountability to reduce risk of exposure and limit liability when and if a breach or a compliance issue arises.

To purchase a DPA tailored for your business, or to create a due diligence plan (including audit materials and best practices), check out the full menu of services available at the [FP U.S. Privacy Hub](#).

Having documented procedures for third-party risk management also reassures regulators and consumers that your business is committed to comprehensive data protection.

4 You Need to Manage Vendors and Third-Party Data Sharing Services



You need robust vendor agreements and monitoring systems to ensure third-party data processors comply with their compliance obligations.



5. Consider the Need for Annual Cybersecurity Assessments

Many privacy laws set minimum security standards (usually a loosely defined standard of adopting reasonable or appropriate security measures tailored to the sensitivity of the data and risk of exposure), but some states like California and Colorado may require assessments for businesses handling certain data types. Conducting annual cybersecurity assessments can serve as a preventative measure, strengthening defenses against data breaches and minimizing the chances of non-compliance.

To inquire about developing or deploying a cybersecurity assessment at your business, check out the [full menu of offerings at the FP U.S. Privacy Hub](#).

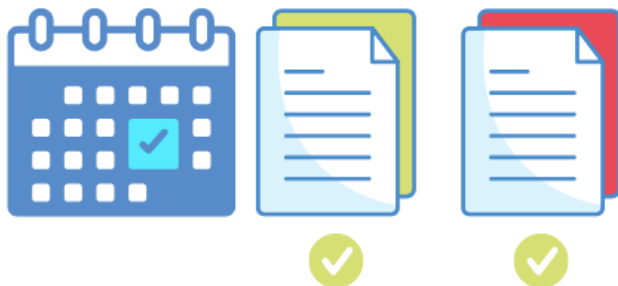
An effective assessment covers areas such as:

- **Encryption Standards** – ensuring data is encrypted both in transit and at rest;
- **Access Control** – defining and monitoring who has access to sensitive data and implementing multi-factor authentication;
- **Vulnerability Management** – routinely scanning for software vulnerabilities and applying security patches;

- **Breach Response Readiness** – establishing protocols to detect, contain, and report data breaches promptly;
- **Network Security** – securing network boundaries with firewalls, intrusion detection systems, and segmentation to limit unauthorized access;
- **Data Minimization** – reducing the amount of personal data collected, stored, and processed to limit exposure;
- **Audit Logging and Monitoring** – recording and reviewing system activity to detect and respond to suspicious behavior;
- **Incident Response Training** – regularly training employees on recognizing threats and following breach protocols;
- **Vendor Security Reviews** – evaluating the security measures of third-party vendors with access to sensitive data; and
- **Backup and Recovery Planning** – implementing regular data backups and testing recovery plans to ensure business continuity.

For businesses handling highly sensitive data, working with external auditors or cybersecurity teams can add a needed layer of security. This work can demonstrate to regulatory bodies that your business is committed to meeting and exceeding compliance standards.

5 Consider the Need for Annual Cybersecurity Assessments



Conducting annual cybersecurity assessments can serve as a preventative measure, strengthening defenses against data breaches and minimizing the chances of non-compliance.



Conclusion

For more tailored resources and ongoing guidance, [our new FP U.S. Privacy Hub](#) offers up-to-date insights, FAQs, and compliance solutions to help you navigate the modern consumer privacy landscape with confidence.

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to [Fisher Phillips' Insight System](#) to get the most up-to-date information direct to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or an attorney on the firm's [Consumer Privacy Team](#).

Related People

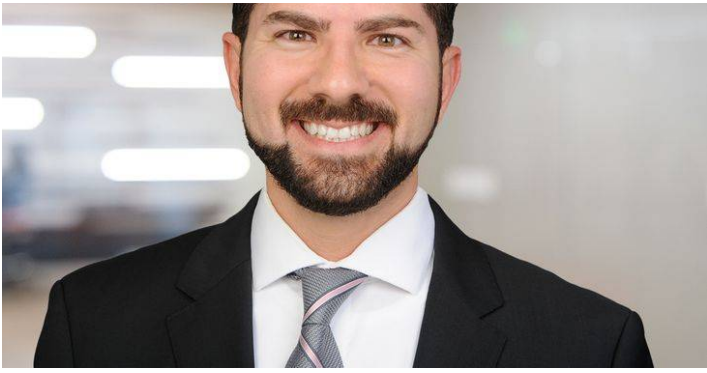


Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
[Email](#)



Kate Dedenbach, CIPP/US
Of Counsel
248.901.0301
[Email](#)





Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Privacy and Cyber
Consumer Privacy Team

Trending

U.S. Privacy Hub