U.S. Consumer Privacy Law Services for Businesses

- Do you feel like a novice when it comes to privacy law compliance – especially with multiple new state laws being enacted?
- Do you feel your business is behind the curve because you don't have a privacy compliance officer or internal expert on privacy law?
- Are you unsure what you would do if you had a data breach tomorrow?
- Are you currently CCPA-compliant but have not yet started on all the other new state laws being enacted?
- Have you reviewed your privacy policies and procedures for compliance with the state laws that have gone into effect in 2024 and those that will be effective in 2025?
- Do you feel good about your CCPA compliance when it comes to non-employee consumers but need help with employment data?
- Do you share data with third parties and need a better handle on managing the data flow?
- Are you interested in conducting a security or privacy assessment but are fearful that doing so without an attorney could lead to the discovery of potentially negative findings?
- Do you have a cyber-insurance renewal coming up and are worried about getting renewed?

If your answer to any of these questions was "yes," the Fisher Phillips Consumer Privacy Team has you covered.

U.S. Consumer Privacy Introductory Packet

This is a solid foundation you need to get started, regardless of your level of experience or expertise. The U.S. Consumer Privacy Introductory Packet includes the following offerings:

1. Compliance Checklist

2. Data Inventory Checklist and Spreadsheet
3. Consumer Notice (aka Privacy Policy)
4. Privacy Policy for Employees (not part of the employee handbook)
5. Notice to Job Applicants

Note: if your data inventory is already complete, the FP Consumer Privacy Team can assist with customizing and developing the required CCPA Notice and Comprehensive Multi-State Privacy Policy based on the previous work you have done.

U.S. Consumer Privacy Compliance Starter Kit

If you're at square one and don't even know where to get started, this package is for you. The Consumer Privacy Compliance Starter Kit gives you everything you need to develop a fully compliant strategy to meet all of your state law privacy needs, including:

1. State Privacy Law Compliance Checklist and Roadmap
2. Data Inventory Checklist & Spreadsheet
3. Notice to Employees
4. Privacy Policy for Employees (not part of the employee handbook)
5. Notice to Job Applicants
6. Notice to Independent Contractors
7. Notice to Individuals in the B-2-B Context
8. Notice to Board Members
9. CCPA Poster for Californians
    - For placement in workplace / physical retail/ office locations
    - This operates as your "offline" notice of collection where personal data may be collected from or about consumers such as through video surveillance or other in-person interaction with a consumer
10. Online Privacy Policy for your public-facing website
11. Data Protection Agreement (DPA)
    - For contracts with your service providers and vendors that process, collect, access, or maintain personal data on your behalf

Note: if your data inventory is already complete, the FP Consumer Privacy Team can assist with customizing and developing the required Notices and Privacy Policy based on the previous work you have done.

Consumer Request Management Kit

This packet is perfect for businesses that collect and store consumer data. In the coming months and years, you are sure to receive consumer requests with respect to that data once the public becomes aware of their rights and enterprising plaintiffs' attorneys poke and prod at various organizations to identify possible deficiencies. By ordering this kit, you'll receive:

1. A consumer request process handbook or manual for managing consumer requests (including methods for receiving requests, your verification process, how to acknowledge requests, a process blueprint for determining who in your organization will respond and what steps they will take with each type of request, and how to maintain proper recordkeeping for compliance)
2. Online Consumer Request Form (which can be used if the law requires you to have an offline paper form available at physical locations or if you are DIY'ing the consumer request process through your website instead of utilizing a software tool)
3. Consumer Request Response Templates (including the standard language and options for responding to different types of consumer requests accounting for different scenarios and options)
4. Script for voicemail greeting message on toll-free number consumers call to submit consumer requests
5. Sample script for employees answering consumer requests on any toll-free phone line

Privacy Training

While California is the only state where there is a requirement to provide training, all managers and employees with responsibility for any part of compliance with state consumer privacy laws benefit from training. Appropriate training can provide robust protection against violations of the laws and, in the event of any missteps, inspire the trust and confidence of regulatory enforcement agencies. You can read more here for a detailed Q&A on this training requirement. By retaining the FP Consumer Privacy Team to host this training, you'll receive:

- An initial one-hour consultation with a member of the FP Consumer Privacy Team to learn about your data privacy and compliance posture, experience, and concerns
- Development and customization of the training material
- An interactive two-hour training session for your executives and managers led by a member of the FP Consumer Privacy Team (either in person or virtual)

The "Jumpstart" Assessment and Data Inventory Program

If you are not sure what your organization needs to get done in order to get into compliance, this program is for you. Our team will provide a workshop to jumpstart your U.S. Consumer Privacy

compliance efforts and tailor an individualized roadmap ahead for you so you can complete your work most efficiently and in a cost-effective manner.

- We offer one-day, three-day, or five-to-six-day programs depending on what's needed at your organization. The best place to start is usually a one-day privacy gap assessment, but we can tack on additional days to focus on an inventory of your employment and other consumer data assets.
- For these programs, we team up with an operational and implementation consulting firm to jointly provide clients with a gap and risk assessment, custom roadmap, and data asset inventory, while maintaining the attorney-client privilege over all communications and work product.
- Each program includes executive-level data privacy training and goal alignment, a tailored privacy risk assessment, and a prioritized 3-6-9-month Privacy Roadmap (tailoring steps to take based on operational needs, risk level, and legal priorities)

Risk Assessment

Although not all state consumer privacy laws require a risk assessment, California, Colorado, Connecticut, Delaware, Montana, Oregon, Tennessee, Texas and Virginia do have such a requirement when specific types of data are being collected. Additionally, the California Privacy Protection Agency has commenced its rulemaking process to cover certain topics the agency did not cover in its first round, including whether businesses subject to the CCPA will be required to conduct an annual "independent" security audit with respect to certain sensitive data for which the risk of exposure and potential harm from exposure are high. For employers, the sensitive and intimate nature of data they collect about employees may trigger the obligation to conduct such an audit.

An annual cybersecurity assessment has been the best practice, but now it will likely become part of many state privacy laws. We strongly recommend this be done on an annual basis. This should be done by an external auditor rather than an internal team evaluating themselves, especially based on the CCPA's use of the term "independent" in describing this annual audit. Moreover, businesses are better served having this audit conducted at the direction of legal counsel to ensure the attorney-client privilege and attorney work product protections will apply.

By retaining the FP Consumer Privacy Team to conduct this assessment for your organization, you'll receive:

- An independent and external audit of all measures across your enterprise to secure and protect all personal information.
- A joint effort by the FP Consumer Privacy Team and a technical cybersecurity expert to provide a legal and technical framework for all advice covered by the attorney-client privilege.

Vendor Management and Due Diligence Assessment

Your relationships with vendors are critical. You will need to make sure that all of your vendor contracts are compliant – as well as ensuring proper due diligence on the part of the vendors so that you are not ensnared in an unintentional data security violation. As part of this assessment, you'll receive the following:

- Since all contracts with vendors and third parties that access, process, or receive any of your consumer data (including any data of your employees or applicants) must be updated to comply with new laws and regulations, you will need to review or rewrite each one. We can draft, revise, and redline your agreements with all such vendors to ensure compliance, with a particular focus on cooperation in responding to consumer requests, obligations and responsibilities in the event of a breach of your data in the vendor's possession, and other similar issues.
- If your company provides services to other entities that include processing, collecting, or maintaining data on their behalf, we can also revise and edit your master services agreement with clients to address compliance from the service provider perspective.
- In addition, the new regulations also require you to include certain terms in contracts with third parties that are not "service providers" (not vendors) with whom you share personal information of any consumers. We'll make sure these contracts are fully compliant.
- We can also step in to directly negotiate terms of data processing agreements with your vendors or their counsel.
- We can also assist with due diligence efforts to ensure the security measures taken by your vendors are sufficient. We may recommend bringing in a cybersecurity consultant to assist with examining the security credentials of your vendors as necessary.
- Finally, if your business clients are requiring you to undergo a security audit or provide documentation of your security measures, we can also work with you on customizing a packet you can provide to your clients in response to such inquiries.

Conclusion

Fisher Phillips will continue to compile guidance for compliance with U.S. state consumer privacy laws. Make sure to subscribe to Fisher Phillips' Insight System to get the most up-to-date information. For further information, contact your Fisher Phillips attorney or any attorney on our Consumer Privacy Team.

Connect with our U.S. Privacy Services Team