nicsa

Consumer Data Privacy Laws Tip Sheet

A best-practices approach to US State Legislation in asset & wealth management.

The current data privacy landscape in the United States is a patchwork of federal laws applicable to certain industries, state breach notification laws, and more recently, state data privacy laws, each with their own requirements. Breach notification laws have been on the books for years, whereas state privacy laws are just beginning to emerge. Firms should have solid practices in place to evaluate new and evolving privacy rules and regulations and solid practices in place to interpret state requirements for breach notifications. This tip sheet will focus on privacy regulations as they relate to consumers or shareholder data.

Many states continue to pursue privacy legislation, the California Consumer Privacy Act of 2018 (the "CCPA"), as amended by the California Privacy Act, is one of the most comprehensive data privacy laws in the United States and an indicator of how privacy legislation is developing in the United States. Inspired by the European Union's General Data Protection Regulation, the CCPA grants California consumers new data privacy rights which will require companies conducting business in California to understand and plan to accommodate. These new data privacy rights provide more transparency and control over personal information that businesses collect. Aside from employee privacy, many of these privacy laws are aimed at firms earning significant revenue from the sale of data, rather than firms collecting data in the ordinary course of conducting their business activities, such as providing investment management and related services to consumers.

With the evolving privacy related regulatory environment, the financial services industry should continue to focus on ensuring compliance with state specific privacy rules and regulations in addition to meeting their obligations under federal law and regulation. Industry groups and firms should focus on monitoring developments in the privacy space at the state and federal levels and be able to react quickly to the ever-changing regulatory environment.

This Tip Sheet contains examples of helpful tips and considerations when evaluating how a state's privacy laws may apply to you. Individual member firms may have their own specific policies and procedures associated with these topics.

1. **Does the law apply to your firm or business activities conducted through various legal entities within your corporate structure? What entities are subject to various state and federal rules and regulations?**

- Legal counsel or publications from law firms may be consulted.
- Is there any relief given within the Gramm-Leach-Bliley Act? Understand scope of your business

activities and what exemptions might apply.
- Be mindful of any data you are collecting for non-customers and may be in scope for state specific privacy laws.
- Any exemption for business to business data at the state level?
- Is there any relief given by number of customers in a state or amount or percentage of revenue derived from data selling activities by the firm? Be mindful of the burden of using these exemptions.
- Review State Ties; consider whether any current fund investors, prospective advisors, employees, or other business contacts are residents of specific states with privacy related guidelines.
- Understand your data collection in general, how is the data stored, who can access it and for how long?
- Understand if your websites are collecting personal information from state residents and how that data is retained. Do you collect cookies?

Determine how business communications are impacted.

- Understand how categories are defined. Ensure you are considering employees, natural persons vs. entities, affiliated persons, directors, contractors, and vendors.
- Understand how opt-out provisions apply, who can give consent, and how that can be managed.
- Know who enforces each state's rules, and who can audit your program and make inquiries.
- Know what penalties or enforcement actions may apply for breaches of the law.
- Know what each state considers to be a "sale" of data. What is not a sale?

2. Determine how any new or amended law or regulation differs from what you are already doing today.

- Things to consider include which law or regulation(s) apply to your firms and designing your program to comply with the most onerous of the requirements that apply. In other words, adopt a single written information security and data privacy program rather than multiple programs that are intended to meet specific individual state or federal requirements.
- You may want to create a chart listing all the legal entities within your corporate structure then identifying which rule or regulation applies to each entity.

3. How do you create a data inventory for your organization? Know this will be a substantial process that includes an understanding of your firm's data management and classification system.

- Categories could range from Public, Internal, Internal personally

identified information (PII), Confidential, Confidential PII, Sensitive PII and Restricted.
- You may want to research data discovery vendor tools that are available.

4. How to define project requirements- what is the work you need to do given what you now know?

- If law dictates special treatment for sensitive PII
- Do you have sensitive PII?
- Are proper controls in place?
- Do you perform automated scans, restrict access rights, have a process in place for vendors?
- Do you provide any opt out choices the law requires?
- What specific data are covered by each state, e.g., geolocation; biometric? What data are excluded, e.g., publicly available data?

5. How do you start the work? (May include system programming, monetary spend may be needed)

- Review and update firm's privacy notice, understand if there are any state specific notices that need to be created.
- Update internal policies and procedures.
- Review Service Provider Agreements. Ensure that the applicable agreements limit the service provider's use of PPI as strictly as the state requires.
- Review relevant insurance coverage and make necessary changes.
- Employee Training. Ensure that personnel responsible for handling consumer inquiries regarding state privacy rights are informed of the applicable requirements and know how to direct consumers to exercise those rights. Develop regular (annual) training for staff.
- Create Processes to respond to consumer requests if required by state law. Have standard state specific responses if needed and understand the potential resource requirements to fulfill the requests. Include times allowed to respond and times allowed to cure.
- Create an Incident Response Plan, some states may have a private right of action and statutory damages for security breaches.
- Collaborate with appropriate internal teams, IT groups, Information Security, Legal, and Compliance. Determine appropriate entitlements to shared folders that may contain PII.
- Create processes for recordkeeping, per state requirements. Include appropriate and regular purge schedules for historical data.

6. How are you going to make sure you stay compliant?

- Who is responsible? – in each line of business and for oversight – do you need a privacy officer/team? Should there be separate privacy officers for technology and business?

- Ensure vendors are in compliance during your periodic reviews of vendors. Rules tend to cover “controller” and “processor” of data. Resources include vendor SOC1’s, standard information gathering questionnaires, and due diligence.
- If you do change vendors understand your compliance needs around data destruction and retention with former vendors.
- Perform internal reviews and testing for adherence, engage internal or external auditors.
- How do you ensure access rights have been done correctly?
- Create a process for ongoing compliance checks.
- Ensuring future state and federal law updates are reviewed.