

The Privacy Parade:

How to Navigate the
Rush of New State
Privacy Laws

July 20, 2023



troutman
pepper

Today's Parade Line-Up



Kim Phan
Washington, D.C.



Josh Davey
Charlotte

State Privacy Laws Timeline

January 1, 2023

- California Privacy Rights Act amendments to the California Consumer Privacy Act
- Virginia Consumer Data Protection Act

July 1, 2023

- California Privacy Rights Act enforcement date
- Colorado Privacy Act
- Connecticut Act Concerning Personal Data

December 31, 2023

- Utah Consumer Privacy Act

July 1, 2024

- Tennessee Information Protection Act

October 1, 2024

- Montana Consumer Data Privacy Act

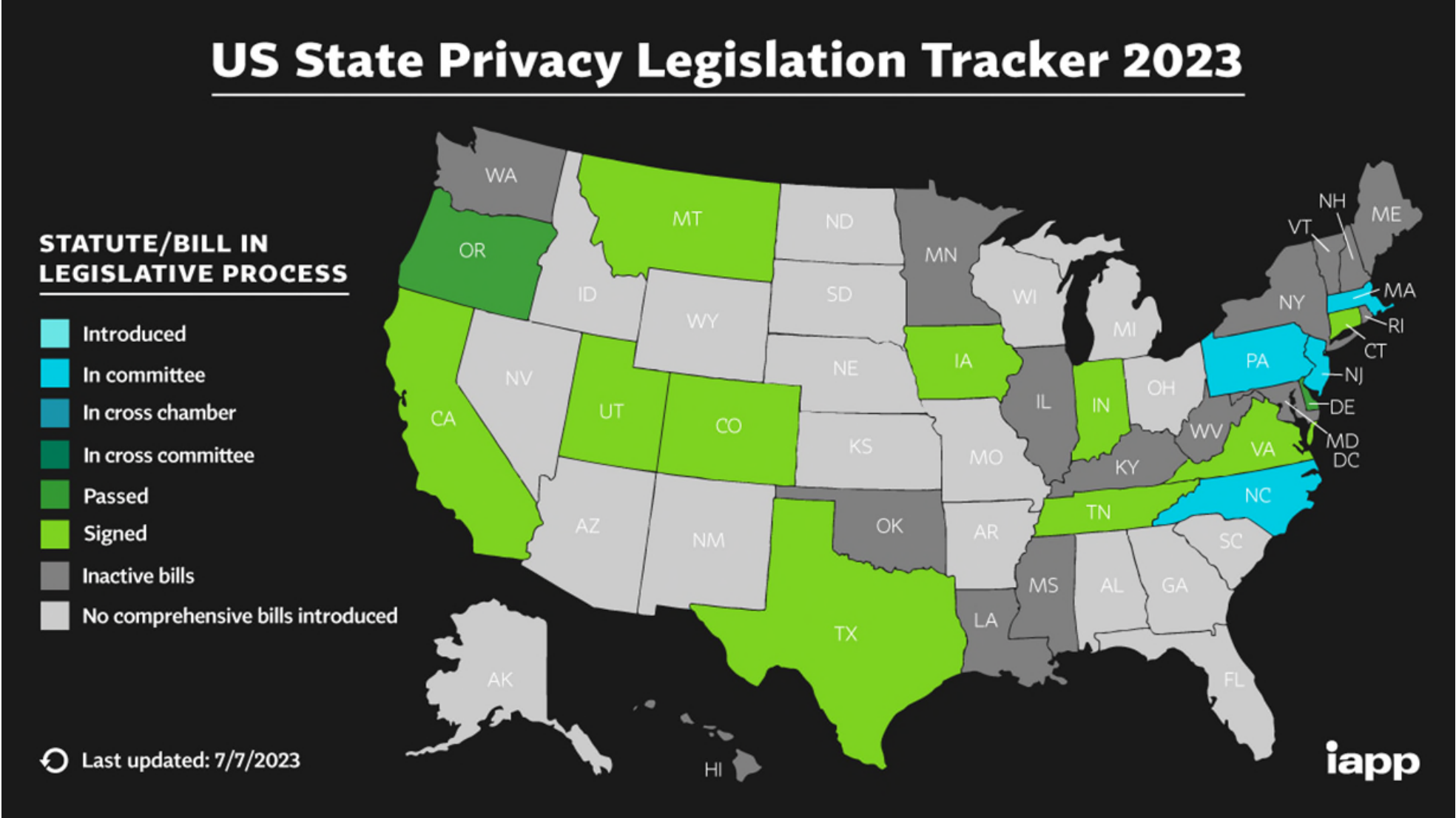
January 1, 2025

- Colorado Privacy Act regulations
- Iowa Consumer Data Protection Act
- Texas Data Privacy and Security Act

January 1, 2026

- Indiana Consumer Data Protection Act

State Privacy Legislation Tracker 2023



Applicability & Business Requirements

Applicability Thresholds

STATE	REVENUE	VOLUME	SALES
California	\$25 million	100,000	50%
Colorado	N/A	100,000	Any sales & 25K
Connecticut	N/A	100,000	25% & 25K
Indiana	N/A	100,000	50% & 25K
Iowa	N/A	100,000	50% & 25K
Montana	N/A	50,000	25% & 25K
Tennessee	N/A	100,000	50% & 25K
Texas	N/A	N/A	Any sales
Utah	\$25 million	\$25 million & 100,000	\$25 million & 50% & 25K
Virginia	N/A	100,000	50% & 25K

Personal Information

California

Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked , directly or indirectly, with a particular consumer or household.

- Identifiers.
- Protected classifications.
- Commercial information, including records of personal property, products or services purchased, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.
- Internet activity, including, browsing history, search history, and ad interactions.
- Geolocation data.



Personal Information

- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information.
- Inferences to create a profile about a consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
- Sensitive personal information.



Personal Information

Other States

- All states exclude:
 - Aggregated
 - Deidentified / pseudonymous
 - Publicly available
- Devices (VA, CO, CT, MT, TN, TX)
- No indirect (except TN)
- No employees
- No business contacts



Exemptions

General exemptions:

Comply with other laws.

Comply with governmental authorities.

Cooperate with law enforcement.

Exercise or defend legal claims.

Data-level exemptions

Gramm-Leach-Bliley Act (financial institutions, affiliates, data)

v.

Fair Credit Reporting Act

Entity-based exemptions:

Health Insurance Portability and Accountability Act (protected health information v. covered entity)

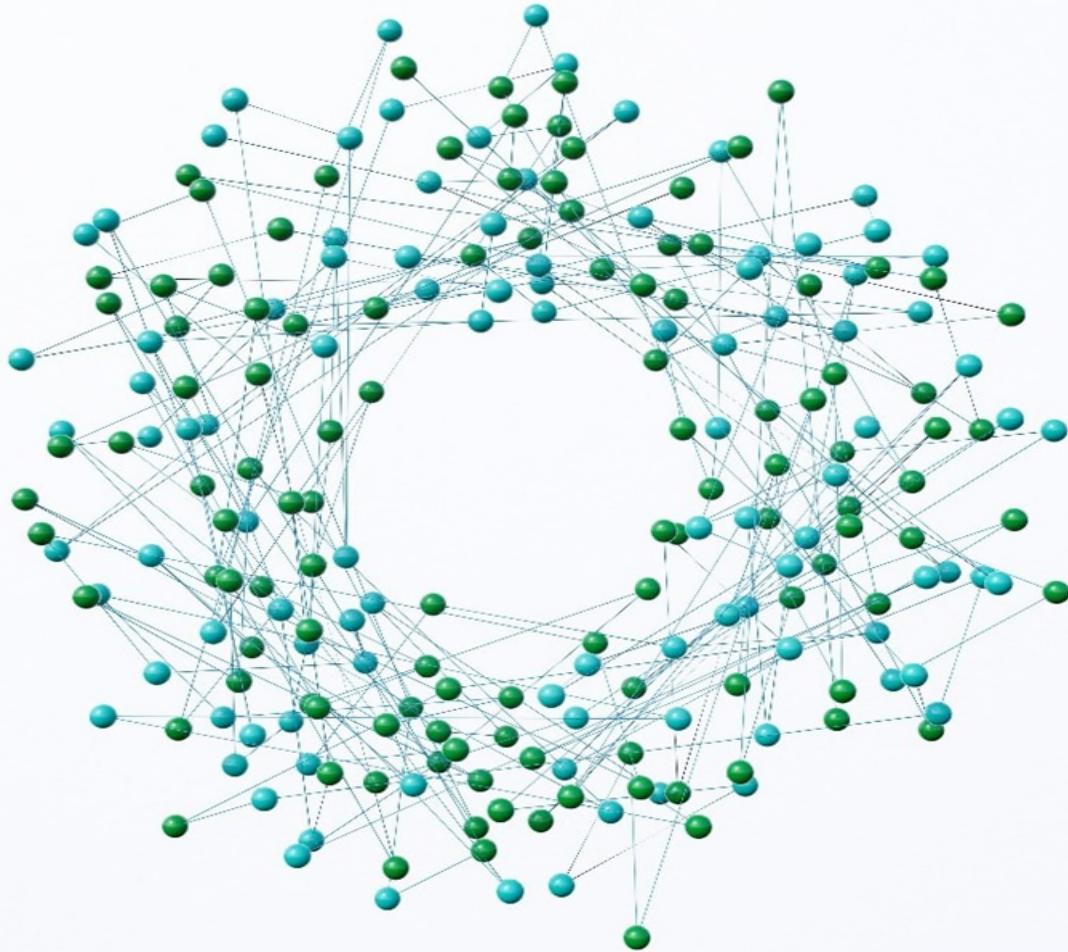
Business Requirements

Privacy disclosures	Consumer rights <ul style="list-style-type: none">• Identity verification• Authorized agents	Data minimization <ul style="list-style-type: none">• Collection, use (secondary use), disclosures, etc.	Consent <ul style="list-style-type: none">(e.g., sensitive, children) / revocation	No discrimination
Data protection assessments <ul style="list-style-type: none">(e.g., sales, targeted advertising, profiling)	Internal policies and procedures	Training	Recordkeeping	Record retention
Data security	Contract provisions	Audits	Deidentification	Automated decision-making

Privacy Policy



Data Mapping



Stakeholders

- Marketing
- Web Development
- HR

Third Parties

- Service Providers
- Contractors

Data Collection Flows

- Selling or Sharing?
- Retention

Key Points

1. Categories of Personal Data

- Consider your audience and any exemptions that may apply

2. Purpose of Processing

3. Categories of Personal Data Disclosed to Third Parties

4. Categories of Third Parties with Whom Personal Data is Disclosed with

- Consider service providers, contractors, and other third parties

5. Exercising Consumer Rights

- Including how to exercise any appeals

6. General Best Practices

- Clear, accessibility, last updated, and contact information



State Specific Nuances

California

- Employee and B2B Data
- Notice at Collection
- Notice of Right to Opt-Out of Sale/Sharing
- Notice of Right to Limit Use of Sensitive Personal Information
- Notice of Financial Incentive



Texas

- Notice of Sale of Sensitive Personal Data
- Notice of Sale of Biometric Personal Data



Consumer Rights – What are States Serving Up?

All States Give Some Flavor Of This:

1. Right to Access
2. Right to Delete
3. Right to Data Portability
4. Right to Opt Out of Sales



Some States Sprinkle On A Little More:

1. Right to Correct
2. Right to Opt Out of Certain Processing
3. Right to Opt In for Sensitive Data Processing
4. Right Against Automated Decision Making



Let's Dig In

Right to access — The right for a consumer to access from a business/data controller the information or categories of information collected about a consumer, the information or categories of information shared with third parties, or the specific third parties or categories of third parties to which the information was shared; or, some combination of similar information.

Right to correct — The right for a consumer to request that incorrect or outdated personal information be corrected but not deleted.

Right to delete — The right for a consumer to request deletion of personal information about the consumer under certain conditions.

Right to opt out of certain processing — The right for a consumer to restrict a business's ability to process personal information about the consumer.

Right to portability — The right for a consumer to request personal information about the consumer be disclosed in a common file format.

Right to opt-out of sales — The right for a consumer to opt out of the sale of personal information about the consumer to third parties.

Right to opt in for sensitive data processing — The right for a consumer to opt in before a business can process their sensitive data.

Right against automated decision making — A prohibition against a business making decisions about a consumer based solely on an automated process without human input.



Snippet above borrowed from the IAPP US State Privacy Legislation Chart, available here:
https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

This Photo by Unknown Author is licensed under [CC BY-ND](https://creativecommons.org/licenses/by-nd/4.0/)

Not All Chocolate Tastes the Same – Issues to Consider




- 1. How does the state define “selling?”**
- 2. What processing activities are regulated?**
 - Profiling
 - Targeted Advertising
 - Activities Resulting in “Legal” or “Similarly Significant” Effects on Individuals
- 3. What exemptions exist?**
 - Entity-level exemptions?
 - Data-level exemptions?

Not All Chocolate Tastes the Same – Issues to Consider



4. **What methods must businesses implement to allow consumers to exercise rights?**
 - Toll-free number? Webform?
 - Opt-Out Preference Signal Required?
5. **What do businesses need to say in privacy notices regarding rights afforded by certain states?**
6. **What rights are afforded to children? How is “child” defined?**
7. **What can businesses do to confirm state of residency?**
8. **Timing considerations?**



Enforcement and Litigation

Enforcing Authority

All States: Enforcement by Attorney General

California: Shared with
CPPA

Colorado: Shared with
District Attorneys

CPPA: Nation's First Dedicated State-Level Privacy Regulator

Governance

- Headed by five-member board
- Two members appointed by governor; one by Assembly Speaker; one by Senate Rules Committee, one by the Attorney General
- One seat currently vacant

Functions

- Promote public awareness of consumers' rights and businesses' responsibilities under the CCPA
- Adopting regulations in furtherance of the CCPA
- Enforce the CCPA beginning July 1, 2023



Cure Periods & Cure Sunsets

30 Days

- Indiana → None
- Virginia → None
- Utah → None

60 Days

- Colorado → 1/1/25
- Connecticut → 1/1/25
- Montana → 4/1/26
- Tennessee → None

90 Days

- Iowa → None

Discretionary

- California

Example Cure Provisions

California: (a) Upon the sworn complaint of any person or on its own initiative, the agency may investigate possible violations of this title relating to any business, service provider, contractor, or person. The agency may decide not to investigate a complaint or decide to provide a business with a time period to cure the alleged violation. In making a decision not to investigate or provide more time to cure, the agency may consider the following: (1) Lack of intent to violate this title. (2) Voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the agency of the complaint. (b) The agency shall notify in writing the person who made the complaint of the action, if any, the agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction.

Example Cure Provisions

Colorado: PRIOR TO ANY ENFORCEMENT ACTION PURSUANT TO SUBSECTION (1)(a) OF THIS SECTION, THE ATTORNEY GENERAL OR DISTRICT ATTORNEY MUST ISSUE A NOTICE OF VIOLATION TO THE CONTROLLER IF A CURE IS DEEMED POSSIBLE. IF THE CONTROLLER FAILS TO CURE THE VIOLATION WITHIN SIXTY DAYS AFTER RECEIPT OF THE NOTICE OF VIOLATION, AN ACTION MAY BE BROUGHT PURSUANT TO THIS SECTION. THIS SUBSECTION (1)(d) IS REPEALED, EFFECTIVE JANUARY 1, 2025.

Iowa: Prior to initiating any action under this chapter, the attorney general shall provide a controller or processor ninety days" written notice identifying the specific provisions of this chapter the attorney general alleges have been or are being violated. If within the ninety- day period, the controller or processor cures the noticed violation and provides the attorney general an express written statement that the alleged violations have been cured and that no further such violations shall occur, no action shall be initiated against the controller or processor.

Penalties

Injunctive Relief

- Available in all states

Penalties Specified in Privacy Law

- California → Up to **\$2,500** per violation; up to **\$7,500 per** intentional violation OR violations involving under 16s
- Connecticut → Up to **\$5,000** per violation
- Indiana, Iowa, Tennessee, Utah, Virginia → Up to **\$7,500** per violation

Penalties Not Specified in Privacy Law

- Colorado → Up to **\$20,000** per violation under Colorado Consumer Protection Act
- Montana → Not specified; up to \$10,000 per violation under Montana Consumer Protection

Private Right of Action (California Only)

Elements

Who can bring: Any consumer

Information covered: Nonencrypted and nonredacted personal information OR usable credentials

Triggering event: Subject to an unauthorized access and exfiltration, theft, or disclosure

Caused by: Violation of duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information

Remedies

Statutory damages \$100-\$750 per consumer per incident OR actual damages, whichever is greater

Injunctive or declaratory relief

Any other relief the court deems proper

No independent basis for attorneys fees, but plaintiffs will seek them under other statutes (e.g., CLRA, UCL).

30-Day Cure

Consumer must provide business 30 days' written notice identifying the "specific provisions" violated

"In the event a cure is possible," Business may provide notice and cut off action for individual or class-wide statutory damages

Implementation of reasonable security practices following a breach is not a cure

Cure period does not apply to claims for actual damages

Sephora USA, Inc. – First CCPA Public Enforcement Action

First public enforcement action under CCPA (August 24, 2022)

\$1.2M settlement with injunctive relief

AG alleged Sephora

- Failed to inform consumers their personal information would be sold when visiting its website and app
- Failed to inform consumers of right to opt out of sale of personal information
- Failed to display a clear “Do Not Sell My Personal Information” link
- Failed to provide two or more methods for submitting opt-out requests
- Failed to treat Global Privacy Control signals as an out-out request
- Continued to sell personal information to third parties despite receiving the Global Privacy Control signal



Sephora USA, Inc. – First CCPA Public Enforcement Action

- Included a claim under California's Unfair Competition Law based on alleged false and misleading statements concerning sale of consumer information and opt-out rights

Lessons

- This is just the beginning
- AG/CPPA will interpret statute broadly
- Focus on opt-out compliance, recognition of Global Privacy Control



Overview of CCPA Litigation to Date

- **Over 300 cases filed invoking CCPA**
- **75% in California; 25% across other jurisdictions**
- **Finance, fintech, software, healthcare, communications, and insurance industry companies are top targets**
- **Small number of plaintiffs' firms responsible for a disproportionate share of litigation**
- **Majority of suits follow data breaches, but some seek to enforce other CCPA rights despite absence of private right of action**
- **CCPA claim frequently paired with common law claims for negligence, unjust enrichment, breach of contract, invasion of privacy and statutory claims under UCL, CLRA, CMIA**
- **Early decisions indicate courts are enforcing scope limitations on private right of action, as well as standing requirements under *TransUnion LLC v. Ramirez***

Regulatory Issues



Colorado Privacy Act

- **Part 1: General Applicability**
- **Part 2: Definitions**
- **Part 3: Consumer Disclosures**
- **Part 4: Consumer Personal Data Rights**
- ***Part 5: Universal Opt-Out Mechanism***
- **Part 6: Duties of Controllers**
- ***Part 7: Consent***
- **Part 8: Data Protection Assessments**
- **Rule 9: Profiling**
- **Part 10: Enforcement**
- **Part 11: Materials Incorporated by Reference**

Colorado Privacy Act – Part 5 (Universal Opt-Out Mechanism)

- **Opt-out mechanism: Consumers may exercise their right to opt out of processing of personal data**
- **Mechanism may allow consumer to opt out of sale of data or use of data for targeted advertising (or both)**
- **Default settings: a Universal Opt-Out Mechanism may not be the default setting for a tool that comes pre-installed on a browser or operating system**
- **Use of personal data collected in connection with use of opt-out mechanism**
- **Technical Specifications**



Colorado Privacy Act – Part 7 (Consent)

- **Consent is required to (1) process sensitive data; (2) processing data concerning a child; (3) selling data, processing data for targeted advertising, or profiling; (4) processing data for purposes not reasonably necessary to or compatible with the original specified purpose.**
- **Requirements for valid consent: (1) it must be obtained through the consumer's clear, affirmative action; (2) it must be freely given by the Consumer; (3) it must be specific; (4) it must be informed; and (5) it must reflect the consumer's unambiguous agreement.**



California Consumer Privacy Act

- **Article 1: General Provisions**
- **Article 2: Required Disclosures to Consumers**
- **Article 3: Business Practices for Handling Consumer Requests**
- **Article 4: Service Providers, Contractors, and Third Parties**
- **Article 5: Verification of Requests**



Article 3: Business Practices for Handling Consumer Requests: *(Requests to Delete, Requests to Correct and Requests to Know)*

- **Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know**
- **Important timelines for responding to requests**
- **Responding to requests to delete, correct, and know**



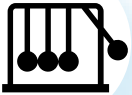
Article 3: Business Practices for Handling Consumer Requests: *(Requests to Opt-out)*

- **Businesses must abide by opt-out preference signals**
- **Businesses that sell or share personal information must provide two or more opt-out methods**
- **Businesses comply by requests to opt-out by ceasing to sell and/or share personal information**
- **Businesses may offer a choice of opting-out of the sale or sharing or personal information**



Closing Thoughts

Six Strategic and Actionable Closing Thoughts

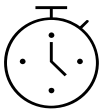


BUILDING BLOCKS – LEVERAGE & BUILD MOMENTUM

If you've built key processes for GDPR or CCPA, **adapt and expand** them. If you're just getting started or still working, **keep going** and ensure your workplan contemplates July 1 deadlines and building beyond the privacy policy.

PRIORITIZE – ENFORCEMENT RISKS

Even the most mature privacy programs have areas that can be enhanced. Prioritize potential risks based on enforcement priorities of regulators that are most relevant to your industry sector and regulatory profile. State AGs that have provided regulatory guidance and been actively communicating enforcement priorities around areas including **targeted advertising, sensitive personal information, children, health data and individual privacy rights**, may begin enforcement on July 1.



IMPLEMENTATION SUCCESS – SCALE, EFFICIENCY, INTEGRATED APPROACH

Data protection is an ongoing process and part of your businesses' lifecycle and value. We can see today that tomorrow looks like more of what we know today. **Don't wait to create or solidify long term plans** to mature your organization's privacy compliance. Begin, or continue to, **raise awareness to get help and secure resources to automate and scale** your work.



3rd PARTY RISK – DOCUMENT YOUR WORK, DEVELOP NEW INTEGRATED DPAs & DPIAs

Many comprehensive state laws (e.g., CA, CO, CT and VA) require **privacy risk assessments (DPIAs)** for high-risk data processing activities. Ensure you have DPIAs in place for activities that involve the use of sensitive personal data, sale of data, ad-tech or profiling. Ensure that you have strong and up-to-date **data protection agreements (DPAs)** in place with your third-party service providers to reflect all new legal requirements including the **Chinese Standard Contract, the latest European SCCs and the UK addendum** (as applicable).



AdTech & CONSUMER EXPERIENCE – DO THE WORK & AUDIT TIME TO TIME

Make certain that your actions are as good as your work. Have you audited your websites to understand what tracking technologies you're using? Are your externally-facing **privacy notices** (including for employees and B2B customers) ready for prime time? Do you have the **correct links and disclosures**? What do consumers experience when they submit a data subject rights request? **Make certain you like what your customers and regulators can see.**



DATA/AI STRATEGY – THINK OUTSIDE THE BOX

Many privacy adjacent data laws are coming online and will affect your overall data strategy and compliance program. Address compliance with new laws in your existing practices in harmony with your core practices and controls. Laws regulating AI such as the EU AI Act, and portions of non-HIPAA health data such as Washington State's MHMDA and NY's similar law will be enforceable in July and if passed, portions of a copy-cat CT law will too. These laws require separate, but compatible policies and practices.

Troutman Pepper Privacy + Cyber

A Collaborative 360-Degree Approach. Troutman Pepper's Privacy + Cyber team extends the range of privacy and cyber services traditionally offered by law firms, drawing upon our unique combination of global expertise in key areas such as privacy program creation and implementation, licensing, financing and M&A transactions, incident response, litigation, and regulatory investigations and enforcement.



Six areas truly differentiate Troutman Pepper's Privacy+Cyber practice:

1. Unique Team and Integrated Suite of Services
2. A Premier Cross-Discipline Firm That Drives Privacy/Cyber Leadership
3. Bespoke Privacy Program Creation, Implementation and Transaction Services
4. Full-Service Incident Response / Cybersecurity Incident Prevention, Response And Recovery Services
5. Industry-Leading Litigation and Risk Mitigation Services
6. Regulatory, Investigations, and Enforcement Defense / Corrective Action Plan Compliance and Monitoring Services



Thank You

Josh Davey / joshua.davey@troutman.com

Kim Phan / kim.phan@troutman.com



troutman
pepper