

U.S. Privacy Laws: All Aboard the Crazy Train

2023 New Legal Risks Symposium

Andrea Maciejewski | Associate

Data Privacy & Cybersecurity Practice, Greenberg Traurig, LLP

maciejewskia@gtlaw.com

SEPTEMBER 20, 2023

www.gtlaw.com

Agenda



I. Overview of Recent and Upcoming U.S. State Privacy Laws



II. Where to Start



III. How to Comply

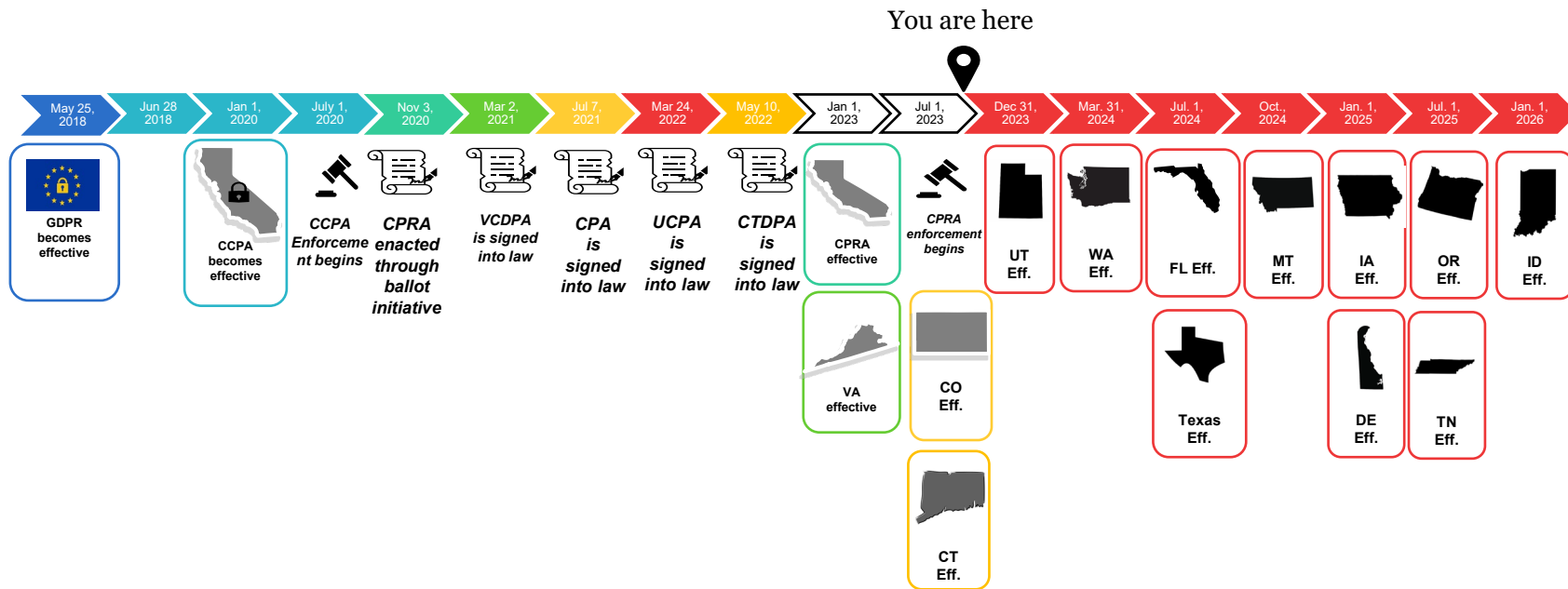


IV. Conclusions and Questions



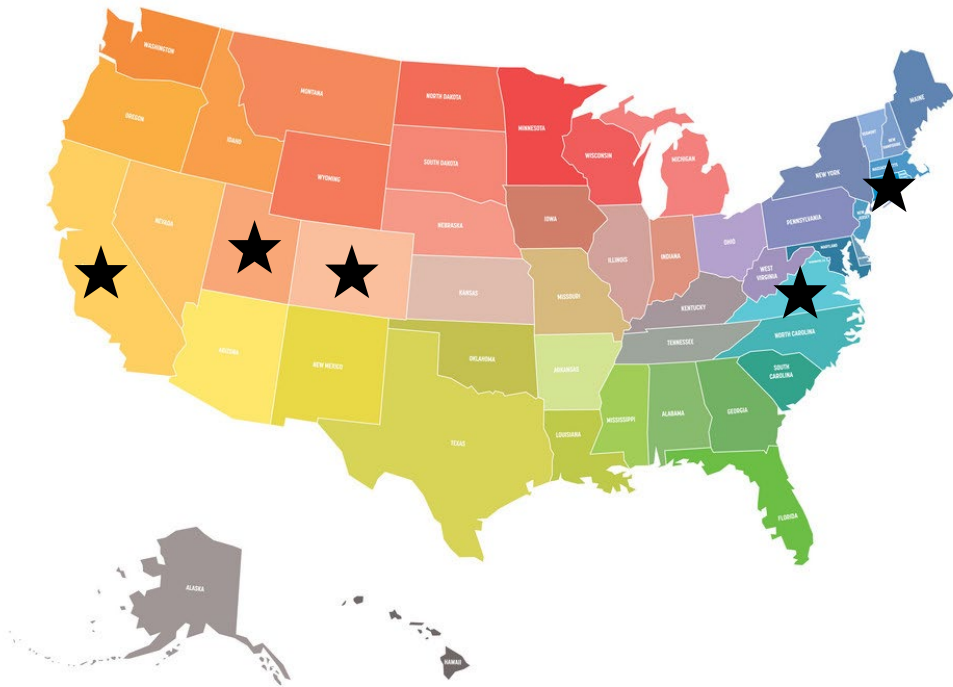
Comprehensive State Privacy Laws (AKA the Wild, Wild West)

Timeline



State Privacy Laws – eff. 2023

- **California Consumer Privacy Act**, *as amended by the California Privacy Rights Act (CCPA)*, eff. 1.1.23, enforced 7.1.23
- **Virginia Consumer Data Protection Act (VCDPA)**, eff. 1.1.23
- **Connecticut Data Privacy Rights Act (CTDPA)**, eff. 7.1.23
- **Colorado Privacy Act (CPA)**, eff. 7.1.23
- **Utah Consumer Privacy Act (UCPA)**, eff. 12.31.23



 UNIVERSITY OF NORTH CAROLINA

- Washington My Health My Data, eff. 3.31.2024
- Florida Digital Bill of Rights, eff. 7.1.2024
- Texas Data Privacy and Security Act, eff. 7.1.2024
- Montana Consumer Data Privacy Act, eff. 10.1.24
- Iowa Consumer Data Protection Act, eff. 1.1.25
- Delaware Personal Data Privacy Act, eff. 1.1.25
- Oregon Privacy Act, eff. 7.1.25
- Tennessee Information Protection Act, eff. 7.1.25
- Indiana Consumer Data Protection Act, eff. 1.1.26

Side-by-Side Comparison

		2018 ^a	2018 ^a	2018 ^a	2018 ^a	2018 ^a	2018 ^a	2018 ^a	2018 ^a	2018 ^a	2018 ^a	2018 ^a	2018 ^a	2018 ^a	2018 ^a	2018 ^a
		California Consumer Protection Act ^a	California Privacy Rights Act ^a	Virginia Consumer Data Protection Act ^a	Colorado Privacy Act ^a	Connecticut Data Privacy Act ^a	Utah Consumer Privacy Act ^a	Washington My Health My Data Act ^a	Florida Digital Bill of Rights ^a	Texas Data Privacy and Security Act ^a	Montana Consumer Data Privacy Act ^a	Delaware Personal Data Privacy Act ^a	Iowa Consumer Data Protection Act ^a	Oregon Privacy Act ^a	Tennessee Information Protection Act ^a	Indiana Consumer Data Protection Act ^a
Acronyms		CCPA ^a	CPRA ^a	VCDPA ^a	CPA ^a	CTDPA ^a	UCPA ^a	WACMDA ^a	EDBR ^a	TDPSA ^a	MCDPA ^a	DDPA ^a	IPA ^a	OPA ^a	TPA ^a	ICDPA ^a
Effective dates		Jan. 1, 2020 ^a	Jan. 1, 2023 ^a	Jan. 1, 2023 ^a	Jul. 1, 2023 ^a	Jul. 1, 2023 ^a (Some 5/1 Oct. 1, 2024) ^a	Dec. 31, 2023 ^a	Mar. 31, 2024 ^a	Jul. 1, 2024 ^a	Jul. 1, 2024 ^a	Oct. 1, 2024 ^a	Jan. 1, 2025 ^a	Jan. 1, 2025 ^a	July 1, 2025 ^a	July 1, 2025 ^a	Jan. 1, 2026 ^a
Scopes	Consumer Data ^a	Yes	Yes	Yes	Yes	Yes	Yes	Yes ^a	Yes ^a	Yes ^a	Yes ^a	Yes	Yes	Yes	Yes	Yes
	HR Data ^a	Deferred ^a	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No
Ability to Process Data ^a	B2B Data ^a	Deferred ^a	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No
	Consent for Processing Sensitive Data ^a	No	Notice & Opt-out ^a	Yes	Yes	Yes ^a	Notice & Opt-out ^a	Yes	Yes ^a	Yes	Yes	Yes	Notice & Opt-out ^a	Yes	Yes	Yes
Individual Rights ^a	Data Minimization ^a	No	Yes ^a (Retention) ^a	Yes ^a (Collection) ^a	Yes ^a (Collection & Retention) ^a	Yes ^a (Collection) ^a	No	No	Yes ^a (Collection & Retention) ^a	Yes ^a (Collection & Retention) ^a	Yes ^a (Collection) ^a	Yes ^a (Collection) ^a	Yes ^a (Collection) ^a	Yes ^a (Collection) ^a	Yes ^a (Collection) ^a	Yes ^a (Collection) ^a
	Notices to Data Subjects ^a	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Accountability & Governance ^a	Financial Incentive Disclosures ^a	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Right to Access ^a	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security ^a	Right to Correction (aka Right to Fix Errors) ^a	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
	Right to Deletion (aka Right to Be Forgotten) ^a	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transfers to Third Parties ^a	Right to Opt-Out of Behavioral Advertising ^a	No	Yes	Yes	Yes	Yes ^a (As of Oct. 1, 2024, CTDPA requires opt-in for those under 18) ^a	Yes	Opt-in with right to withdraw consent ^a	Yes	Yes	Yes	Yes	Yes ^a	Yes	Yes	Yes
	Right to Opt-Out of Sales ^a	Yes	Yes	Yes	Yes	Yes	Yes	Opt-in with right to withdraw consent ^a	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Affirmative Defenses ^a	Right to Opt-Out of Profiling & Automated Decision Making ^a	No	To be addressed by regulations ^a	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
	Right to Limit Use of Sensitive Information ^a	No	Yes	No	No	No	Yes	No	Yes	Yes	No	No	Yes	No	No	No
Transferers to Third Parties ^a	Right to Appeal ^a	No	No	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Right to Nondiscrimination ^a	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Affirmative Defenses ^a	Honor opt-out signals (E.g., GPC) ^a	Yes ^a	Yes	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No
	Data Protection Assessments ^a	No	Yes ^a (To be addressed by regulations ^a)	Yes	Yes	Yes ^a	No	No	Yes	Yes	Yes	Yes ^a	No	Yes	Yes	Yes
Transferers to Third Parties ^a	Appropriate Data Security to Safeguard Information ^a	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Breach Notifications ^a	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transferers to Third Parties ^a	Contractual Requirements in Service Provider Agreements ^a	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Other ^a	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Adherence to NIST Privacy is an affirmative defense ^a

Recap



14 state privacy laws



9 different “effective”
dates



Over 350 pages of law
not including regulations

And they are all different...



Where to Start?

What Laws Apply to You?

Initial Vetting Questions:

1. Do you do business in the state?
2. Do you target/market to residents of the state?
3. Do you have information about more than 100,000 individuals in that state (50k in MT or 35k in DE)?
4. Do you sell data (e.g., to a data broker) and have information about more than 25,000 individuals in that state?
5. Do you have annual revenues of over \$25m? (TN, CA, UT)

These questions are not determinative! Some laws require more (FL, TN) and some less (TX, MT, DE). **If you meet even one of these thresholds for any state, you should either check the law or engage privacy counsel to confirm applicability.**

Exception to Applicability

Exceptions vary, but they *may* include:

Non-profits

B2B

Employee data

GLBA and FCRA data or covered entities

HIPAA data or covered entities

Who is Going to Run the Show?



PRIVACY COMPLIANCE
OFFICER



GENERAL COUNSEL



OUTSIDE COUNSEL

What Do You Already Have in Place?



Privacy policies (consumer or employee)



Marketing rules (e.g., how to let people opt out of emails)



Security policies



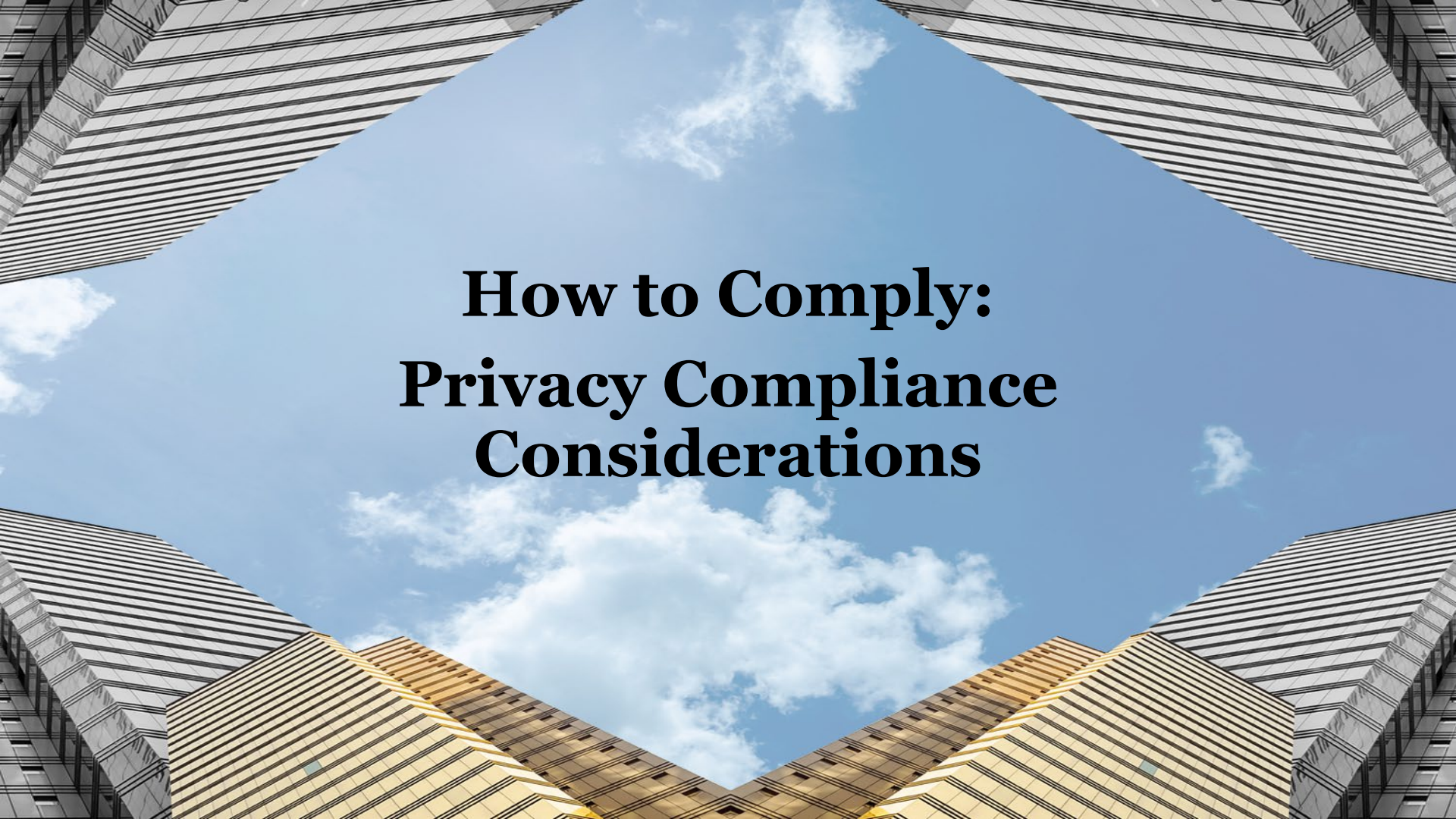
Data breach procedures



Record retention and destruction procedures



Anything else relating to your records or your data

A low-angle, upward-looking perspective of several modern skyscrapers. The buildings are constructed with a grid-like facade of windows and structural elements. The sky is a clear, vibrant blue, dotted with soft, white cumulus clouds. The composition creates a sense of height and architectural grandeur, with the buildings' lines converging towards the top of the frame.

How to Comply: Privacy Compliance Considerations

Key Elements of Privacy Compliance



**Ability to Process
Data**



**Notice &
Transparency**



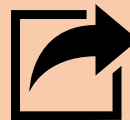
Individual Rights



Security



**Accountability &
Governance**



**Transfers to Third
Parties**

Ability to Process Data: Key Questions

When are we allowed to collect data?

What do we need to do in order to collect the data?

What are we allowed to do with the data once we have it?

How long are we allowed to keep the data?

When Can You Collect the Data?

- **Purpose of Processing** – Companies should collect data for a specific, identifiable purpose.
- **Purpose Limitation** - Companies should not process personal information for “secondary purposes” (i.e., purpose that are neither reasonably necessary to nor compatible with the disclosed purposes for which the data is processed), unless they obtain consent.
- **Consent to process sensitive personal information** - Some state privacy laws (e.g., VA, CO, CT) require companies to obtain an individual’s consent before they can process sensitive personal information.

What Constitutes Consent?

- Consent must be “freely given, specific, informed, and unambiguous.”
- Some states (e.g., CA, CO, and CT) expressly prohibit the use of “dark patterns.”
- “**Dark pattern**” is “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.” (CA, CO, CT)
 - CT also includes “any practice the Federal Trade Commission refers to as a ‘dark pattern’.”

How Long Can You Keep the Data?

- **Data Minimization** – Companies should limit the collection of personal information to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed.
- **Record Retention** – Companies should document the appropriate length of time that records should be retained.
- **Record Destruction** – Companies should destroy any records that are no longer needed.

Notice & Transparency

Under all the comprehensive state privacy laws, companies are required to provide individuals with a “reasonably accessible, clear, and meaningful privacy notice.”

General Requirements (i.e., common across states)

- Categories of PI collected (including sensitive PI)
- Purpose for collecting/processing PI
- Categories of PI shared with third parties
- Categories of third parties to whom PI is shared
- Whether PI is sold
- Whether PI is used for targeted advertising
- A description of a consumer’s rights
- Method for submitting rights requests

Notice & Transparency – Tips

- Because many of the state laws have overlapping disclosure requirements, companies should consider posting/providing a single consolidated consumer-facing privacy notice instead of creating a separate notice for data subjects in each state whose law applies to the company.
- Because a company's data collection and processing practices may differ with respect to the personal information of consumers versus employees and other staff, companies should consider maintaining a separate privacy notice for employees and contractors.

Individual Rights

- There is considerable overlap amongst the state laws regarding individual privacy rights.
- However, some rights are not granted by all states with comprehensive privacy laws.
- Notably, California extends privacy rights to job applicants and employees.



Individual Rights

- Access
- Portability
- Deletion
- Correction
- Opt-out of profiling
- Limit the Use of Sensitive Information
- Nondiscrimination
- Non-discrimination
- Opt-out of Sale
- Opt-out of Sharing

Security

- Most laws require “reasonable security measures”
- What is reasonable?



Accountability & Governance

Data Protection Impact Assessments (DPIA)

- Some states (**VA, CO, CT, FL, TX, MT, DE, OR, TN, IN**) require companies to conduct a data protection assessment (also referred to as a data protection impact assessment) when processing personal information that presents a “heightened risk of harm,” including:
 - Processing personal information for purposes of targeted advertising
 - Selling personal information
 - Processing sensitive data
 - Processing personal information for certain forms of profiling
- DPIAs are formal documents whose primary purpose is to describe how the benefits to the company, the consumer, and the public that flow from the processing activity weigh against the potential risks to the rights of the consumer associated with such processing.



Transfers to Third Parties

- All of the comprehensive state privacy laws require businesses/controllers to enter into contracts with entities to whom they transfer personal information.
 - Most of the state laws (e.g., CPA, CTDPA, UCPA, and VCDPA) only have one category of recipients called **data processors**.
 - The CCPA establishes three categories of recipients – **service providers**, **contractors**, and **third parties** – and sets forth a baseline set of prohibitions that must be contractually addressed when businesses sell or share PI to such entities.
- 
- A close-up photograph of a red pen with gold-colored accents resting on a document. The document has the word 'CONTRACT' printed in large, bold, black letters at the top. Below the title, there is a section titled 'THIS AGREEMENT made this' followed by a line for a date and 'day of'. Further down, there is a section titled 'WITNESSETH: That in consideration' followed by a line for a sum of money and 'lawfully performed on the day of'. At the bottom, there are lines for 'said party of the first part' and 'said party of the second part' with corresponding names and addresses. The document is slightly blurred, and the pen is in sharp focus.



Contract Requirements for Transfers to Processors/Service Providers

- ✓ Instructions for processing
- ✓ Nature and purpose of processing
- ✓ Duration of processing
- ✓ Rights and obligations of both parties
- ✓ Ensure that each person processing personal data is subject to a duty of confidentiality
- ✓ At controller's direction, delete or return all personal data at the end of the of services, unless retention of is required by law
- ✓ Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with its obligations
- ✓ Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor
- ✓ Engage any subcontractor pursuant to a written contract to meet the obligations of the processor with respect to the personal data

Transfers to Third Parties – Tips

- A company may include the data processing terms as an addendum to their services agreement with the vendor or as a standalone agreement. Attaching these terms as an addendum may be more efficient when the company has a master services agreement with the vendor governing multiple statements of work.
- A company should develop procedures for regularly auditing its vendor agreements for compliance with these requirements, especially considering the frequency with which new laws and regulations concerning these requirements are being enacted/promulgated.

BONUS!!

Tracking Tech and Targeted Advertising

- Cookies (i.e., small files placed on a website visitor's device) and other tracking technologies such as beacons, pixels, and tags enable a variety of features and functionalities, including serving targeted ads based on a user's online behavior measured over time and across different websites.
- Tracking technologies used for targeted advertising may be placed by third parties when a user visits the company's site (third-party trackers) in addition to trackers placed by the company itself (first-party trackers).
- All of the comprehensive state laws confer upon data subjects the right to opt out of targeted advertising.

Tracking Tech and Targeted Advertising

- Properly effectuating this opt-out right generally requires placing in the website footer (1) a link labeled “Do Not Sell or Share My Personal Information” or “Your Privacy Choices” through which users may indicate that they do not want their information shared for targeted advertising and possibly (2) a cookie settings link that expands to a portal where the user may indicate their preference to not have targeted advertising and/or other types of trackers (e.g., analytics trackers) deploy when they use the site.
- Under the CPRA regulations, California has created strict technical requirements for the implementation of this opt-out right with which it is very difficult (practically impossible) to fully comply. As such, companies subject to the CCPA might want to consider implementing an opt-in strategy where advertising trackers do not deploy until a user indicates his or her preference to allow such trackers (e.g., by clicking accept on a banner that drops on initial page load).





Questions?