Compliance with New and Upcoming U.S. Privacy Laws

Presented by:

Karin E. Ross | RossK@gtlaw.com | Associate, Data Privacy & Cybersecurity Practice, Greenberg Traurig, LLP (Denver, CO)

Talia Boiangin | Talia.Boiangin@gtlaw.com | Associate, Data Privacy & Cybersecurity Practice, Greenberg Traurig, LLP (Orlando, FL)

SEPTEMBER 13, 2023

GT GreenbergTraurig

Agenda

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

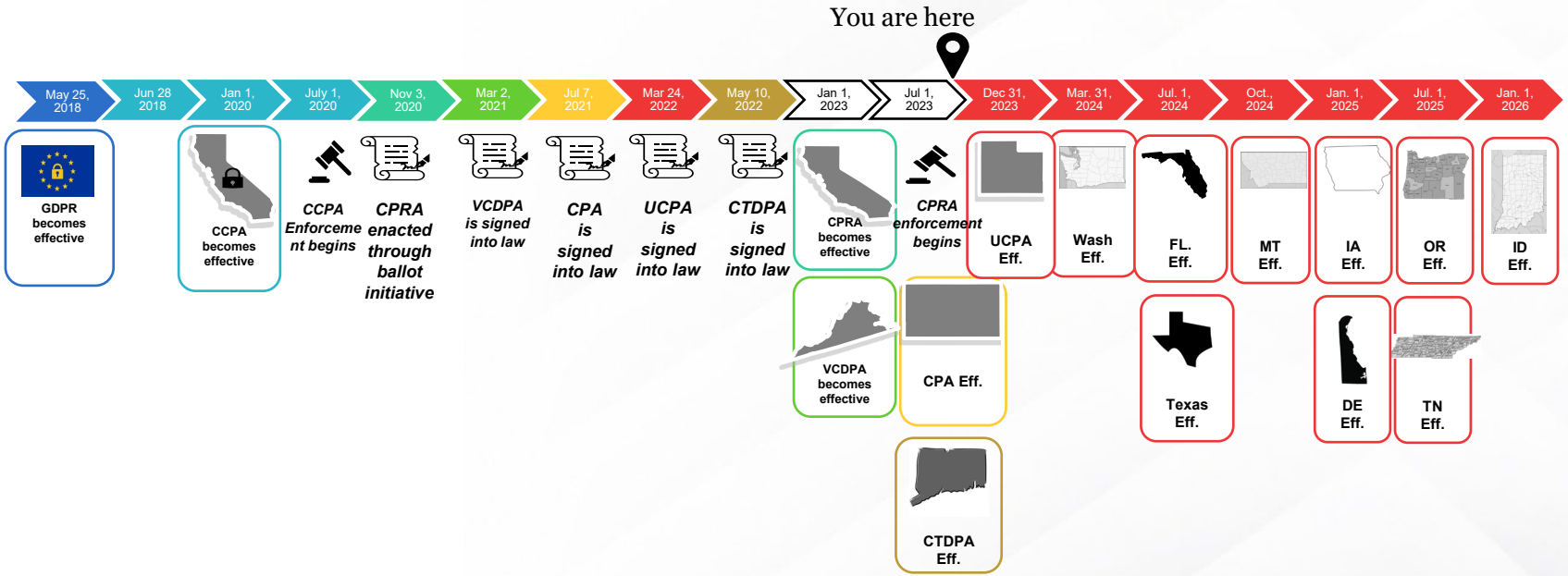
II. Privacy Considerations for Organizations

IV. Conclusions and Questions

Comprehensive State Privacy Laws

GT GreenbergTraurig

Timeline



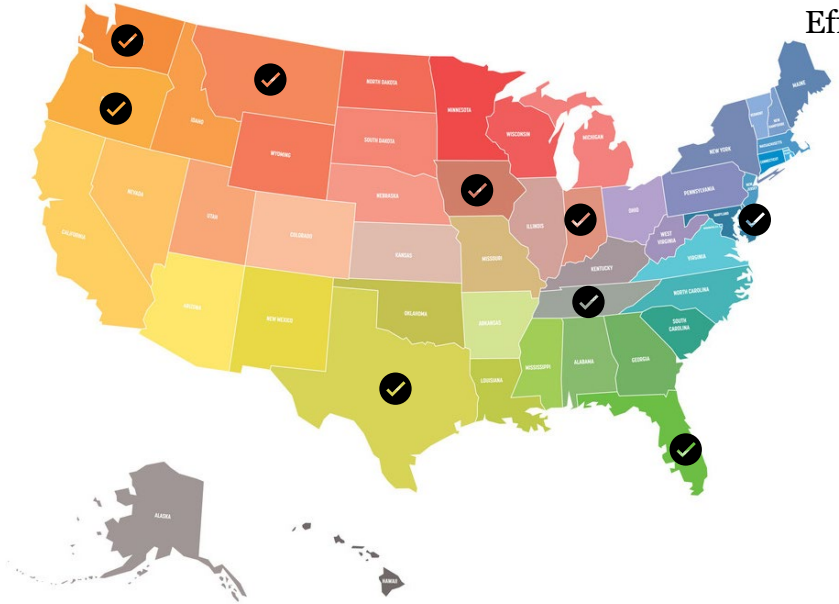
GT GreenbergTraurig

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

GT GreenbergTraurig

Privacy Legislation – Enacted 2023



Effective 2024+

- **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

GT GreenbergTraurig

Florida Digital Bill of Rights (FDBR)

- **Effective Date: July 1, 2024** … but the section requiring data protection assessments for certain activities (e.g., processing for targeted advertising) applies to processing activities occurring on or after **July 1, 2023**.
- **Scope:** Applies to for-profit businesses that (1) conduct business in Florida or produce a product or service used by Florida residents, and (2) process or engage in the sale of personal data, except in a commercial or employment context.

Seems broad, right?

GT GreenbergTraurig

Florida Digital Bill of Rights (FDBR)
Scope Limitation

- The class of businesses to which the FDBR applies is significantly narrowed by its definition of "controller."
- Under the FDBR, a "controller" is a legal entity that:
  - (1) is for profit, conducts business in Florida, and directly or indirectly collects personal data about "consumers" (i.e., Florida residents not acting in a commercial or employment context);
  - (2) alone or jointly determines the purposes and means of processing personal data about consumers;
  - (3) has an annual gross revenue exceeding **$1 billion**; **and**
    - (a) derives at least 50% of its global gross revenue from selling online ads, including providing targeted advertising; **or**
    - (b) operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud-computing service that uses hands-free verbal activation; **or**
    - (c) operates an app store or digital distribution platform offering at least 250,000 different software applications for download and installation by consumers.

GT GreenbergTraurig

Florida Digital Bill of Rights (FDBR) Enforcement

- The Florida Department of Legal Affairs has the authority to enforce violations as an unfair and deceptive practice.
- 45-day period to cure violations after notification.
- Civil penalty of up to $50,000 per violation or triple that amount if:
  - (1) The violation involves a Florida consumer under 18 years of age.
  - (2) The entity fails to delete or correct applicable personal data.
  - (3) The entity continues to sell or share the consumer's personal data after the consumer chooses to opt out of such sale or sharing.
- No private right of action.

GT GreenbergTraurig

Side by Side Comparison

		2020	2023					2024				2025				2026
		California Consumer Protection Act	California Privacy Rights Act	Virginia Cons. Data Protection Act	Colorado Privacy Act	Connecticut Data Privacy Act	Utah Consumer Privacy Act	Washington My Health My Data	Florida Digital Bill of Rights	Texas Data Priv. and Sec. Act	Montana Consumer Data Privacy Act	Delaware Personal Data Privacy Act	Iowa Consumer Data Prot. Act	Oregon Privacy Act	Tennessee Information Protection Act	Indiana Consumer Data Prot. Act
Acronym		CCPA	CPRA	VCDPA	CPA	CTDPA	UCPA	WMHMDA	FDBR	TDPSA	MCDPA	DPDPA	IPA	OPA	TIPA	ICDPA
Effective date		*Jan. 1, 2020*	*Jan. 1, 2023*	*Jan. 1, 2023*	*Jul. 1, 2023*	*Jul. 1, 2023 (Some ₵'s Oct. 1, 2024)*	*Dec. 31, 2023*	*Mar. 31, 2024*	*Jul. 1, 2024*	*Jul. 1, 2024*	*Oct. 1, 2024*	*Jan. 1, 2025*	*Jan. 1, 2025*	*July 1, 2025*	*July 1, 2025*	*Jan. 1, 2026*
Scope	Consumer Data	✓	✓	✓	✓	✓	✓	✓ *(Only Consumer Health)*	✓ (only certain businesses see §)	✓ (only certain businesses see §)	✓	✓	✓	✓	✓	✓
	HR Data	*deferred*	✓													
	B2B Data	*deferred*	✓													
Ability to Process Data	Consent for Processing Sensitive Data		*Notice & Opt-out Norm*	✓	✓	✓	*Notice & Opt-out Norm*	✓	✓	✓	✓	✓	*Notice & Opt-out Norm*	✓	✓	✓
	Data Minimization		✓ *(Retention)*	✓ *(Collection)*	✓ *(Collection & Retention)*	✓ *(Collection)*			✓ *(Collection & Retention)*	✓ *(Collection & Retention)*	✓ *(Collection)*	✓ *(Collection)*	✓	✓ *(collection)*	✓ *(Collection)*	✓ *(Collection)*
Individual Rights	Notices to Data Subjects	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Financial Incentive Disclosure	✓	✓		✓											
	Right to Access	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Right to Correction *(aka Right to Fix Errors)*		✓	✓	✓	✓			✓	✓	✓	✓		✓	✓	✓
	Right to Deletion *(aka Right to Be Forgotten)*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Right to Opt-Out of Behavioral Advertising		✓	✓	✓	✓ *(As of Oct. 1, 2024, CTDPA requires opt-in for those under 18)*	✓	*Opt-in with right to withdraw consent*	✓	✓	✓	✓	✓	✓	✓	✓
	Right to Opt-Out of Sale	✓	✓	✓	✓	✓	✓	*Opt-in with right to withdraw consent*	✓	✓	✓	✓	✓	✓	✓	✓
	Right to Opt-Out of Profiling & Automated Decision Making		*To be addressed by regulation*	✓	✓	✓			✓	✓	✓	✓		✓	✓	✓
	Right to Limit Use of Sensitive Information		✓				✓		✓				✓			
	Right to Appeal			✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓
	Right to Nondiscrimination	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Honor opt-out signals (E.g., GPC)	✓	✓		✓	✓				✓	✓	✓		✓		
Accountability & Governance	Data Protection Assessments		✓ *To be addressed by regulation*	✓	✓	✓			✓	✓	✓	✓		✓	✓	✓
Security	Appropriate Data Security to Safeguard Information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Breach Notification	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*	✓*
Transfers to Third Parties	Contractual Requirements in Service Provider Agreements	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Affirmative Defenses																*Adherence to NIST Privacy is an affirmative defense*

Privacy Compliance Considerations

GT GreenbergTraurig

Key Elements of Privacy Compliance

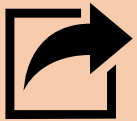
Ability to Process Data

Notice & Transparency

Individual Rights

Security

Accountability & Governance



Transfers to Third Parties

GT GreenbergTraurig

Ability to Process Data

- **Purpose Limitation -** Companies should not process personal information for "secondary purposes" (i.e., purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the data is processed), unless they obtain consent.
- **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.

GT GreenbergTraurig

Ability to Process Data

- **Consent to process sensitive personal information -** Some state privacy laws (e.g., VA, CO, CT, WA, FL, TX, MT, DE, OR, TN, IN) require companies to obtain an individual's consent before they can process sensitive personal information.
  - CA, UT, and IA are unique in that they require "clear notice and an opportunity to opt-out of the processing" of sensitive personal information.

GT GreenbergTraurig

What is "Sensitive" Information?

- Sensitive information is a subset of personal information that includes:
  - Racial origin
  - Ethnic origin
  - National origin (OR only)
  - Religious beliefs
  - Philosophical beliefs (CA only)
  - Trade union membership (CA only)
  - Citizenship or citizenship status (CO, CT, DE, FL, IN, IA, MT, OR, TN, TX, UT, VA only)
  - Immigration status (CT, DE, FL, IN, IA, MT, OR, TN, TX, UT, VA only)
  - Genetic data
  - Biometric information
  - Health (mental or physical) information
  - Sexual orientation
  - Sex life (CA, CO, CT, DE, MT, TN only)
  - Sexuality (TX only)
  - Transgender or non-binary status (OR, DE only)
  - Personal data from known child (VA, CO, CT, DE, FL, IN, IA, MT, OR, TN, TX only)
  - Precise geolocation (CA, CT, DE, FL, IN, IA, MT, OR, TN, TX, UT, VA only)
  - Social Security/Tax ID number (CA only)
  - Driver's License/Gov. ID number (CA only)
  - State ID card number (CA only)
  - Passport number (CA only)
  - Account Log-in + security/password (CA only)
  - Financial account number + security/password (CA only)
  - Credit card number + security/password (CA only)
  - Debit card number + security/password (CA only)
  - Contents of email/mail/text (if business is not intended recipient) (CA only)
  - Health insurance information + name (CA only)
  - Military ID number + name (CA only)
  - Victim status (CT, OR only)

GT GreenbergTraurig

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.'"

GT GreenbergTraurig

Notice & Transparency

- Under all the comprehensive state privacy laws, companies are required to provide individuals with a "reasonably accessible, clear, and meaningful privacy notice."
  - ***Privacy Notice*** *(aka* ***Privacy Policy****) typically describes an organization's data processing practices, including how the organization collects, uses, retains and discloses personal information.*

GT GreenbergTraurig

Notice & Transparency

General Requirements (i.e., common across states)	California-Specific Requirements
• 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	• Categories of sources from which the PI is collected • Categories of PI disclosed for a business purpose • Categories of PI sold • Business or commercial purpose for collecting or selling PI • Retention periods • Financial incentive disclosure

GT GreenbergTraurig

Notice & Transparency

- **Practical 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.
    - *Note that additional state-specific sections may be created for states with particularly idiosyncratic requirements that do not apply to other states (such as California's requirement to disclose categories of information collected and the third parties to whom information is disclosed with reference to statutorily enumerated categories).*
  - 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.

GT GreenbergTraurig

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.

GT GreenbergTraurig

Individual Rights

- **Access** – All of the current state privacy laws generally give consumers a right to access their PI.
  - Trade secrets are explicitly excluded in CO, CT, CA, DE, and OR.
  - Extremely broad (i.e., applies to any PI the controller is "processing.")
  - CA also requires additional disclosures (e.g., categories and specific pieces of PI collected; (ii) categories of sources from which PI is collected; (iii) purpose for collecting or selling PI and (iv) categories of third parties with whom the business shares PI for the last 12 months. DE also requires disclosing categories of third parties with whom the business shares PI, while OR requires a specific list.
- **Portability** (i.e., the right to obtain a copy of PI in a portable and readily usable format that allows the consumer to transmit data to another controller without hindrance).
  - Only consumer-provided PI (VA and UT).
  - Any PI the business/controller has concerning the consumer (CA, CO and CT). DE and OR afford this right but explicitly exclude trade secrets.
- **Deletion** – All of the current state privacy laws give consumers the right to delete their PI.
  - Only consumer-provided PI (CA and UT).
  - Any PI the business/controller has concerning the consumer (VA, CO, CT, DE, and OR).
  - All of the new state privacy laws have numerous exceptions to the right to deletion.
- **Correction** – Most of the current state privacy laws give consumers a right to correct inaccurate PI.
  - Only UT does not provide this right.

GT GreenbergTraurig

Individual Rights

- **Confirmation of Processing** – Less than half of states with passed privacy laws afford this right (VA, CO, CT, DE, OR, and UT).
  - Trade secrets are explicitly excluded in DE and OR.
- **Appeal a Decision Regarding a Request** – While not a right per se, some states require businesses to allow consumers to appeal a decision when the business denies the request of another right.
  - Only VA, CO, CT, DE, and OR afford this to consumers.
- **Opt-Out of Sale** – All of the current state privacy laws give consumers a right to opt-out of sales.
  - Some states (e.g., CA, CO, CT) have a very broad definition of "sale" that includes the exchange of personal data for monetary *or other valuable* consideration.
- **Opt-Out of Targeted Advertising/Sharing** – All of the current state privacy laws give consumers a right to opt-out of targeted advertising/sharing.
  - CA uses the term "sharing for purposes of cross-context behavioral advertising" whereas the other states use the term "targeted advertising."

GT GreenbergTraurig

Individual Rights

- **Opt-out of profiling/automated decision-making** – Most of the current state privacy laws give consumers a right to opt-out of "profiling in furtherance of decisions that produce legal or similarly significant effects."
  - Only UT does not provide this right.
- **Limit the use/disclosure of sensitive PI**– Only CA* affords the right to limit the use and disclosure of sensitive PI.
  - UT and IA are unique in that they require notice and the right to opt-out of processing sensitive PI.
- **Nondiscrimination** – All of the current state privacy laws prohibit businesses/controllers from discriminating against consumers who exercise their privacy rights (i.e., denying access to, charging different prices for, or providing different qualities of goods or services).
  - CA is the only state that gives consumers a *right* to non-discrimination. The other states simply prohibit it.

GT GreenbergTraurig

Security

- CA: Businesses must implement ***reasonable security procedures and practices*** appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure.
- CT, VA: Controllers must establish, implement, and maintain ***reasonable administrative, technical, and physical data security practices*** to protect the confidentiality, integrity, and accessibility of personal data…appropriate to the volume and nature of the personal information at issue.
- CO: Controllers must take ***reasonable measures to secure personal data*** during both storage and use from unauthorized acquisition. The data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business.
- UT: Controllers must establish, implement, and **maintain reasonable administrative, technical, and physical data security practices** designed to (i) protect the confidentiality and integrity of personal data; and (ii) reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data. Considering the controller's business size, scope, and type, a controller shall use data security practices that are appropriate for the volume and nature of the personal data at issue.

GT GreenbergTraurig

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
- In CA, CPPA is working on regulations, but they are not finalized.

GT GreenbergTraurig

Accountability & Governance

- DPIAs are formal documents that are meant to identify, analyze, and minimize the risks associated with certain processing activities.
- Their 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.
- DPIAs must also describe the safeguards that the company employs to reduce those risks.
- States that obligate or will obligate companies to conduct DPIAs (VA, CO, CT, FL, TX, MT, DE, OR, TN, IN) require these documents to be made available to the relevant regulator upon request.

GT GreenbergTraurig

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.

GT GreenbergTraurig

Transfers to Third Parties

- Contracts must meet specific requirements, including:
  - ✓ Instructions for processing
  - ✓ Nature and purpose of processing
  - ✓ Type of data subject to 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

GT GreenbergTraurig

Transfers to Third Parties

Requirements under the CCPA:

- General Requirements (Service Provider, Contractor, and Third Party)
  - ✓ Specifies PI disclosed only for limited and specified purposes.
  - ✓ Obligates recipient to comply with applicable obligations and provide the same level of privacy protection required under the CCPA.
  - ✓ Grants the business rights to take reasonable and appropriate steps to help ensure that the PI is used in a manner consistent with the business's obligations under the CCPA.
  - ✓ Requires recipient to notify the business if it determines it can no longer meet its statutory obligations.
  - ✓ Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of PI.

- Additional Service Provider or Contractor Requirements – all of the above, **plus:**
  - ✓ Must prohibit contractor/service provider from: (1) using, retaining, or disclosing PI for any purpose other than to perform business purpose(s) or outside of the business relationship; (2) selling or sharing PI; (3) combining PI from difference sources.
  - ✓ Contractor/service provider to notify business of sub-processors and bind sub-processors by written contract to the same obligations.
  - ✓ Requires contractor/service provider to permit business to audit/monitor compliance ("may" used in relation to service providers).
  - ✓ Contractors must certify their understanding of and compliance with the contractual requirements (but not required for service providers).

GT GreenbergTraurig

Transfers to Third Parties

- **Practical 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.

GT GreenbergTraurig

Best Practices

- ✓ ***Website***: Make sure your public-facing materials are compliant with applicable laws.
- ✓ ***Data Inventory***: Have a clear understanding of the data you collect, share, and retain; document processing activities; follow retention/destruction policy.
- ✓ ***Sensitive Data***: Identify and ensure sensitive data processing activities are in line with applicable laws and undertake/document DPIAs as required.
- ✓ ***Contracting***: Vet vendors processing personal information on your behalf, and make sure contract provisions (indemnification/LOL) provide sufficient protection.
- ✓ ***Documentation***: Like the GDPR, the U.S. state privacy laws are about documentation that shows the organization is aware of the laws' compliance requirements and making a good-faith effort to comply.

GT GreenbergTraurig

Questions?

Karin Ross

RossK@gtlaw.com

Talia Boiangin

Talia.Boiangin@gtlaw.com