



---

**PROGRAM MATERIALS**  
**Program #32211**  
**September 22, 2022**

# **California Privacy Rights Act - Understanding Your New HR and B2B Compliance Obligations**

**Copyright ©2022 by**

- **Darren Abernethy, Esq. - Greenberg Traurig, LLP.**
- **Gretchen Ramos, Esq. - Greenberg Traurig, LLP.**

**All Rights Reserved.**  
**Licensed to Celesq®, Inc.**

---

**Celesq® AttorneysEd Center**  
**[www.celesq.com](http://www.celesq.com)**

**5301 North Federal Highway, Suite 150, Boca Raton, FL 33487**  
**Phone 561-241-1919**

# CPRA PRIVACY



## Understanding Your HR and B2B Compliance Obligations

Gretchen A. Ramos [ramosg@gtlaw.com](mailto:ramosg@gtlaw.com) 415.655.1319

Darren Abernethy [abernethyd@gtlaw.com](mailto:abernethyd@gtlaw.com) 415.655.1261

## Speakers



Gretchen Ramos, CIPP/US/E, CIPM  
Global Co-Chair – Data  
Privacy & Cybersecurity Group  
Greenberg Traurig LLP  
San Francisco, California  
415.655.1319 | ramosg@gtlaw.com



Darren Abernethy, CIPP, PLS, FIP  
Shareholder – Data, Privacy &  
Cybersecurity Group  
Greenberg Traurig LLP  
San Francisco, California  
415.655.1261 | abernethyd@gtlaw.com

# Agenda

---

1. Current CCPA Obligations - HR and B2B Data
2. Organizations Subject to the CPRA
3. Compliance Obligations
  - a) Notice
  - b) Individual Rights
  - c) Contracting
  - d) Risk Assessments & Security Audits
  - e) Data Breach
  - f) Enforcement
  - g) B2B - Website
4. Compliance Checklist



# CCPA – Current HR & B2B Obligations

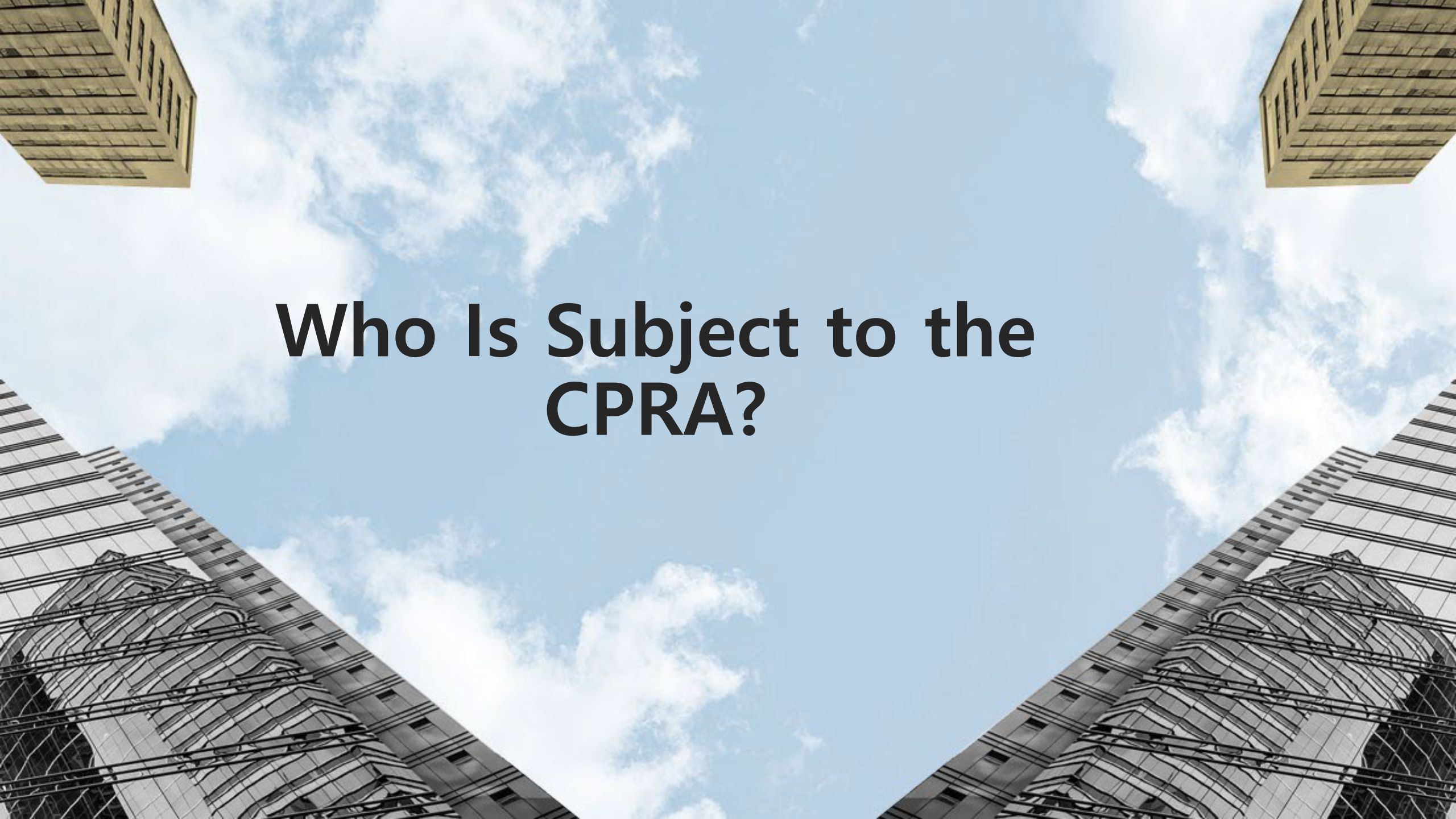
## 1798.145(h)(1) – Employee Exemption

CCPA

- ✓ CCPA generally does not apply to personal information collected by a business about employees, job applicants, or owners, when that “information is collected and used by the business solely within the context of”:
  - (1) the individual’s role as an employee, job applicant, owner, etc.,
  - (2) maintaining emergency contact information, and
  - (3) the administration of benefits.
- ✓ Section 1798.100(b) notice requirements still apply so California employees and job applicants must be presented a notice of collection or a privacy policy. Also, employees still have a private right to sue in data breach matters (i.e., when involving “nonencrypted and nonredacted personal information”).

## 1798.145(n)(1) – B2B Transactions

- ✓ CCPA does not apply to personal information collected by a business about an individual, when the individual is acting as an employee on behalf of their employer in the context of “providing or receiving a product or service to or from” the business.

A low-angle, upward-looking photograph of several tall skyscrapers against a bright blue sky filled with scattered white clouds. The buildings are positioned at the corners of the frame, creating a sense of height and scale. The central area of the image is dominated by the text.

# Who Is Subject to the CPRA?

# SCOPE

## CPRA – Business Definition

1. For-profit legal entity that collects consumers' PI and that determines the purposes and means of processing, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year or

(B) Alone or in combination, annually **buys, sells, or shares** the personal information of **100,000** or more consumers or households or

(C) Derives 50 percent or more of its annual revenues from selling or **sharing** consumers' personal information.

2. Any entity that **controls or is controlled by a business**, as defined in paragraph (1), and that shares **common branding** with the business and with whom the **business shares consumers' personal information**.

3. A **joint venture or partnership** composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

4. A person that does business in California, that is not covered by paragraph (1), (2), or (3) and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.

## CCPA – Business Definition

1. For-profit legal entity that collects consumers' PI and that determines the purposes and means of processing, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), or

(B) Alone or in combination, annually **buys, receives for the business's commercial purposes, sells, or shares** for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices, or

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

2. Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business.

# Why Should You Care About the CPRA?

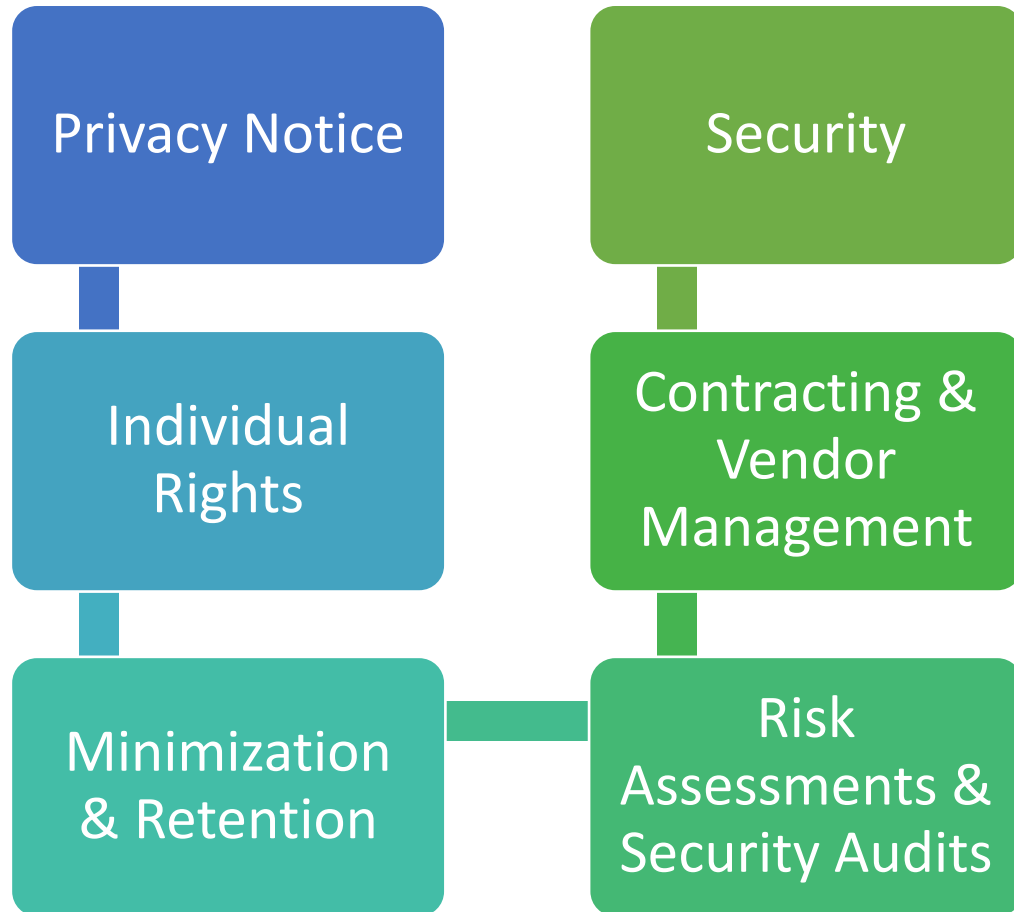
- **Heavy Lift.** Under CPRA, HR and B2B data are subject to **ALL** of the law's various data protection obligations.
- **Enforcement.** California Privacy Protection Agency (CPPA) is the first dedicated privacy regulator in the U.S., with a \$10M annual budget to wit, so likely more enforcement is coming.
- **Fines** = \$2,500 per violation; \$7,500 per intentional violation.
- **No Grace Period.** 30 day cure period under CCPA eliminated as of January 1, 2023.





# CPRA Compliance Obligations

# Overview



# CPRA Notice Requirements

*CalOPPA also requires disclosures regarding the use of third-party tracking technologies and confirming whether or not the service honors “Do Not Track” signals.*

- A list of the categories of personal information the company has collected about consumers in the preceding 12 months.
- Identification of the categories of sources from which the personal information is collected.
- A list of the categories of personal information it has disclosed for a business purpose in the preceding 12 months by reference.
- A list of the categories of personal information it has sold or shared about consumers in the preceding 12 months.
- Categories of third parties to whom the information was shared or sold.
- Sensitive Personal Information - the types of SPI collected, purpose of collection, and whether SPI shared or sold
- A description of a consumer’s rights, as well as details on how a consumer or its authorized agent can submit a rights requests.
- The length of time the business will retain each category of personal information, or where this is impossible, the criteria used to determine such period.

# CPRA Individual Rights

- ✓ **Right to Access.** Consumers may request access to a copy of specific information, including (i) 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.
- ✓ **Right to Delete.** Businesses are required to delete (upon request) any PI that the business has collected “from the consumer” if an exception does not apply. Businesses must direct service providers to delete the PI from their records. notify third parties to delete any consumer PI bought or received, subject to certain exceptions.
- ✓ **Right to Correction.** Consumers may request any correction of their PI held by a business if that information is inaccurate.
- ✓ **Right to Opt Out of Use of “Sensitive PI.”** Consumers may limit the use and disclosure of sensitive PI for certain “secondary” purposes, including prohibiting businesses from disclosing sensitive PI to third parties, subject to certain exemptions.
- ✓ **Right to Opt Out of Automated Decision-Making Technology.** Consumers may opt out of automated decision-making technology, including “profiling,” in connection with decisions related to a consumer’s work performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
- ✓ **Right to Access Information About Automated Decision Making.** The CPRA authorizes regulations which will allow consumers to make access requests seeking meaningful information about the logic involved in the decision-making processes and a description of the likely outcome based on that process.
- ✓ **Right to Nondiscrimination.**
- ✓ **Right to Opt Out of Behavioral Advertising/Selling.**
- ✓ **Opt-In Rights for Minors.**



# Delete Me!

---

- Methods for submitting deletion requests.
- Response times (e.g., CA requires confirmation of receipt of request within 10 business days, but all states require full response within 45 days with a possible 45 day extension if notified).
- Processes such as backup, archive, offline storage, etc. What is “deletion”?



# Deletion Exceptions

The CPRA contains various exceptions to deletion requirement including the following relevant to employees:

- (1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
- (7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information.
- (8) Comply with a legal obligation.

# CPRA – Contractual Requirements



CPRA seeks to protect PI as it flows from businesses to (a) service providers, (b) contractors and (c) third parties.

- Third Party Contracts

- Agree to use limitation and CPRA compliance
- Agree to allow business to audit third party to ensure processing is compliant with CPRA, and business can take appropriate steps to remediate unauthorized use of PI
- Requires third party to notify business if it can no longer meet CPRA obligations

- Contractor and Service Provider Contracts

All of the above must be included, **plus** contract provisions that

- Prohibit the use, retention or disclosure of PI for any purposes than to perform the specific services (business purpose(s))
- Prohibit further selling or sharing PI
- Prohibit retaining, using or disclosing PI outside of the direct business relationship between the service provider and the business
- Prohibit combining PI from different sources
- Assist the business through appropriate technical and organizational measures in complying with the requirement to implement reasonable security procedures and practices.
- Assist the business in responding to a verifiable consumer request
- Agree to notify the business of sub-processors
- Agree to bind sub-processors by written contract to the same obligations
- Agree 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)

# Vendor Management

Employers should:

- Identify service providers and third parties that receive your employee or applicant personal information (e.g., payroll companies, health/benefits/wellness providers, HR consultants, staffing agencies, etc.).
- Conduct vendor inquiries and diligence about how they use, share and secure the employee personal information.
- Enter into agreements with service providers, contractors, and third parties containing specific terms including:
  - Specify the personal information is disclosed by the business only for limited and specific purposes
  - Obligate the service provider to comply with applicable CPRA obligations and provide the same level of privacy protection as is required of them under the CPRA
  - Requires service provider to notify the business if it makes a determination that it can no longer meet its obligations under the CPRA
  - Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information



# CPRA – Reasonable Security Measures, etc.



- RSM. Requires adoption of “reasonable security procedures and practices appropriate to the nature of the PI” to protect it from unauthorized access, use or disclosure.
- S&I. Added new definition for “Security and integrity” to harmonize with GDPR’s “appropriate technical and organization measures” language. S&I means the ability of:
  - (1) Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.
  - (2) Businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions.
  - (3) Businesses to ensure the physical safety of natural persons.
- Data Breaches. The CCPA/CPRA do not impose data breach reporting obligations, as that is covered under a separate notification law. However, a private right of action for any CA consumer (including employees and B2B contacts) does still apply, and not just in relation to “non-encrypted and non-redacted personal information,” but also...



# CPRA – Data Breach

CPRA expands breach liability subject to a private right of action and statutory damages to failures to reasonably protect an individual's email in combination with a password or security question and answer permitting access to an online account (login credentials).

Recall too, statutory damages apply.

# CPRA – Risk Assessments & Security Audits



- Risk Assessment. CPRA requires a business engaged in "significant risk" processing to file with the CPPA on a regular basis a risk assessment with respect to their processing of PI, including:
  - whether the processing involves sensitive PI, and
  - identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with such processing, with the goal of restricting or prohibiting such processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.
- Cybersecurity Audit. Regulations also forthcoming regarding:
  - When a business is required to perform an annual cybersecurity audit because their processing presents a "significant risk" to privacy or security.
  - Defining the scope of the audit and establishing a process to ensure that audits are thorough and independent.
  - Factors to be considered in determining when processing may result in significant risk to the security of personal information.
    - Seems likely that businesses that collect "sensitive personal information" under the CPRA's new definition will fall within audit requirement because of adverse consequences of a breach.

# Enforcement



## 30 Day Cure Period – Now Ailing

- CCPA's provision providing that a business may avoid a violation and administrative fines if it cures any alleged violation within 30 days after being notified of any alleged noncompliance has been eliminated.
- However, still applies where business found not to have reasonable security measures, but a data breach does not occur.

## Fines

- \$2,500 per violation.
- \$7,500 per intentional violation or a violation involving a consumer under 16.

## Draft Regs

- Provide guidance for filing a sworn complaint with the enforcement agency.
- Outline how the Agency shall conduct “probable cause hearings” which require notice to the alleged violator before conducting hearing where it makes a “probable cause determination.
- Empower the Agency to audit businesses to ensure compliance with the CPRA.

# B2B Operations – Now in Scope



**CPRA compliant privacy notice for B2B PI processing activities**



**Description in privacy policy to where employees of other business can assert rights**



**If sharing/selling cookies firing on website, add necessary selling/sharing opt out link to website**



**If sensitive PI collected, add limit use of sensitive PI link to website, with corresponding mechanisms and back-end processes**



*No dark patterns*



# Website & Mobile App Compliance

- The CPRA maintains the CCPA's "sale" definition and adds a new definition for "sharing" PI, which involves "cross-contextual behavioral advertising."
- Big implications for the use of 3<sup>rd</sup> party trackers on websites or 3<sup>rd</sup> party SDKs/integrations on mobile.
- Operational changes re: "Do Not Sell or Share My Personal Information" links and supporting tools and/or web forms.
- This may also necessitate contractual updates with ad tech/martech vendors to clarify roles (e.g., note that the proposed CPRA regs exclude the possibility of a "service provider" being engaged in sharing or CCBA).
- User-enabled opt-out preference signals and global privacy controls!



# HR & B2B Checklist

*Get Cracking  
Now*



# CPRA HR & B2B Compliance Checklist

---

- ❑ **Step 1: Scope.** Determine if you are a “business” under the CPRA.
- ❑ **Step 2: Team.** Identify the members of the team that will lead the CPRA HR & B2B compliance projects.
- ❑ **Step 3: Data Inventory.** Create or update organization’s data inventory to ensure it fully identifies all HR and B2B PI that your organization’s is processing and sharing; be sure to identify any sensitive personal information being processed.
- ❑ **Step 4: Data Minimization.** Assess data processing activities and establish internal controls (e.g., policies or procedures) to ensure that you collect only PI that is adequate, relevant, and reasonably necessary in relation to the purposes disclosed to consumers.
- ❑ **Step 5: Contracting.** Identify, review and to the extent necessary, reach out to vendors, services providers and third parties to put in place compliant CPRA contract provisions / addendums.
- ❑ **Step 5: Rights Requests.** Create procedures and defensible guidelines on how organization will be responding to HR and B2B rights requests.
- ❑ **Step 6: Website.** If you are a B2B business, review and update your website to come in line with do not sell, do not share, sensitive personal information opt-out, and GPC requirements.
- ❑ **Step 7: Privacy Notices.** Revise and update your employee and job candidate privacy notices to come in line with CPRA; make sure your current privacy notice includes any B2B processing activities or draft a stand-alone privacy notice for B2B processing.
- ❑ **Step 8: Retention.** Determine the period of time that HR and B2B will be retained and create or update your organization’s data retention and destruction policy.
- ❑ **Step 9: Risk Assessment/Security Audit.** If your organization engages in high-risk processing activities, perform and document a risk assessment and/or security audit. *CPRA to provide guidance.*
- ❑ **Step 10: Training.** Update training materials, implement procedures for training and conduct training.





# QUESTIONS



**Gretchen A. Ramos**  
[ramosg@gtalw.com](mailto:ramosg@gtalw.com)  
415.655.1319

**Darren Abernethy**  
[abernethyd@gtlaw.com](mailto:abernethyd@gtlaw.com)  
415.655.1261