

Preparing Your Business for the California Privacy Rights Act



Scott C. Hall

Partner

shall@coblentzlaw.com



Mari S. Clifford

Associate

mclifford@coblentzlaw.com

California Privacy Rights Act of 2020

(Proposition 24)

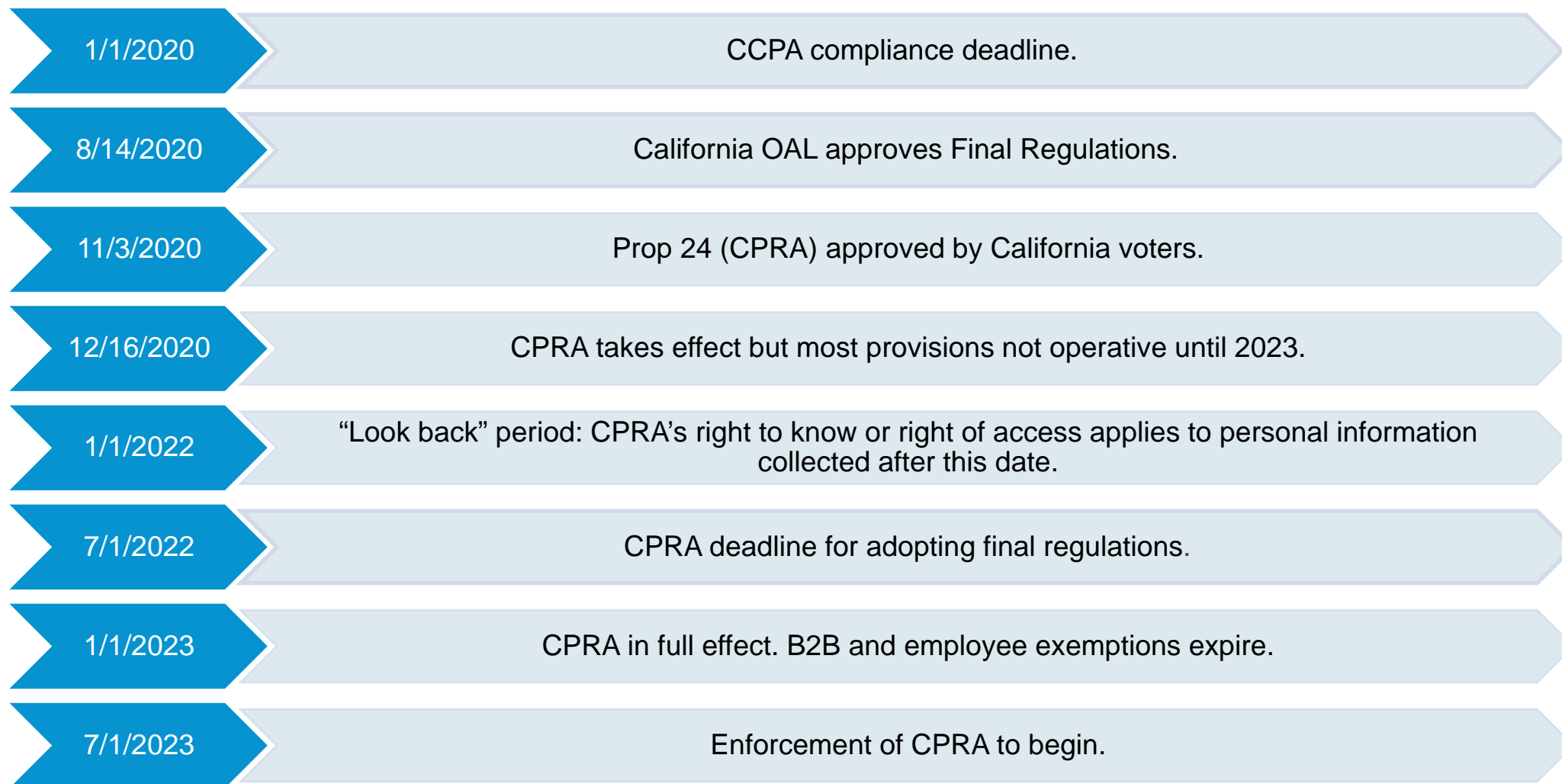


"I'm updating my privacy policy."



© marketoonist.com

California Privacy Rights Act (CPRA)



CCPA and CPRA: How are they related?

CPRA is an amendment of the California Consumer Privacy Act (CCPA). It expands on several areas of the existing CCPA.

The California Office of the Attorney General will retain civil enforcement authority over the CCPA and CPRA.

Businesses who have thus far avoided or ignored CCPA obligations should immediately get in compliance for a few reasons:

- It is the law in California and will be enforced.
- The CCPA contains a private right of action—and plaintiff’s lawyers are already actively filing suit.
- The CPRA, if viewed in the context of augmenting a business’s existing compliance framework or building a program from scratch, is a “CCPA+”.

TRUE or FALSE?

A federal data privacy law will be passed that will save my business from having to comply with the CPRA.

FALSE
(for now)

There are ongoing discussions about a federal data privacy law, but it will likely take a few years to enact a comprehensive federal law.

TRUE or FALSE?

Our business is CCPA and/or GDPR compliant, nothing more is needed to comply with CPRA.

FALSE

GDPR/CCPA compliance efforts will likely help CPRA compliance, but the laws are not identical and the obligations imposed on businesses require different actions to comply.

DOES THE CPRA APPLY TO MY BUSINESS?

Let's find out!

Applicability of the CPRA


The CPRA maintained most of the CCPA definitions with a few notable exceptions.

CPRA narrowed the definition of “businessess” covered by the privacy act and introduced new concepts of “sharing” information as liable as well.


“Business”

- A sole proprietorship, partnership, limited liability company, corporation, or other legal entities organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers’ personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California, and that meets one of the three thresholds described below;

Applicability (cont.)



As of January 1 of the calendar year, had a granular gross revenue in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year.



Alone or in combination, annually **buys, sells, or shares** for cross-context behavioral advertising the personal information of **100,000** or more consumers or households, or



Derives 50 percent or more of its annual revenues from selling or sharing behavioral advertising consumers' personal information.

***Only one of the three must be met for the CPRA to apply.**

Applicability (cont.)

The CPRA maintains the CCPA's categories of personal information (PI) but adds the new subcategory of "sensitive personal information."

Personal Information

1. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
2. Any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.
3. Characteristics of protected classifications under California or federal law.
4. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
5. Biometric information.
6. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
7. Geolocation data.
8. Audio, electronic, visual, thermal, olfactory, or similar information.
9. Professional or employment-related information.
10. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
11. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Applicability (cont.)

Sensitive Personal Information

1. Social security, driver's license, state identification card, or passport number;
2. Account log-In, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
3. Precise geolocation;
4. Information regarding a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
5. The contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication;
6. Genetic data;
7. The processing of biometric information for the purpose of uniquely identifying a consumer;
8. Personal information collected and analyzed concerning a consumer's health; or
9. Personal information collected and analyzed concerning a consumer's sex life or sexual orientation

Selling Personal Information

What is “selling” information under the CCPA?

- “Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, **disclosing**, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party **for** monetary or other **valuable consideration**.
- Any disclosure of data for valuable consideration.
- Cloud storage providers, HR/payroll services, advertising, email service providers?

Sharing Personal Information

The CPRA also introduced limitation on “sharing” personal information.

“Sharing”

- Refers to a business’s disclosure of personal information to a third party for “cross-context behavioral advertising,” regardless of whether the disclosure is also a “sale.”
- **“Cross-context behavioral advertising”** is defined as the “targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.”

In essence, this definition intends to capture the collection of a consumer’s personal information across third-party digital properties for the purposes of *targeted advertising*.

- Under the CPRA, consumers have a separate right to opt-out of “sharing” personal information.
- A business must advise consumers of this new right through a clear and conspicuous link on the business’s homepage titled “Do Not Sell or Share My Personal Information.” This link replaces the current “Do Not Sell My Personal Information” link required by the CCPA.



Consumer Rights Under the CPRA (Modified CCPA Rights)

Right to Delete	Businesses are now required to notify third parties to delete any consumer PI bought or received, subject to some exceptions.
Right to Know	The PI that must be reflected in a “Right to Know” response is expanded to include PI collected beyond the prior 12 months, if collected after January 1, 2022.
Right to Opt Out	The opt-out right now covers “sharing” of PI for cross-context behavioral advertising as outlined below.
Opt in Rights for Minors	Extends the opt-in right to explicitly include the sharing of PI for behavioral advertising purposes. As with the opt-out right, businesses must wait 12 months before asking a minor for consent to sell or share his or her PI after the minor has declined to provide it.
Right to Data Portability	Consumers may request that the business transmit specific pieces of PI to another entity, to the extent it is technically feasible for the business to provide the PI in a structured, commonly used and machine-readable format.

Consumer Rights Under the CPRA (cont.)

(New Rights)

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 Automated Decision Making Technology	The CPRA authorizes regulations allowing consumers to opt out of the use 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 allowing 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 Restrict 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.

Relationships with External Entities

Service Providers

- Service providers remain entities that process personal information on behalf of a business pursuant to a written contract.
- CPRA clarifies, however, that a service provider may receive the personal information either *directly from* or *on behalf of* the business.

Third Parties

- A third party continues to be a recipient of sales of personal information.
- A third party that offers cross context behavioral advertising can now be the recipient of “sharing” of personal information, as well.

New Term: Contractors

- “Contractor” refers to a person to whom the business makes available a consumer’s personal information for a business purpose and pursuant to a written contract. In particular, **contractors are required to certify their understanding and compliance with contractual restrictions.**
- Contractors are nearly identical to service providers, with just two differences: contractors are not data processors; and contractors must make a contractual certification in CCPA contracts.

Business Obligations

1. Data Minimization

2. Expanded Notice Obligations

3. Updating service provider agreements and third party contracts regarding disclosure and personal information

4. Updating privacy policy and related compliance systems

5. Implementing “reasonable security measures”

6. Audit Obligations

Notice Obligations

Required notices to consumers:

1. Notice at Collection
2. Notice of Right to Opt Out of Sale and Sharing
3. Notice of Right to Limit Use of Sensitive Personal Information
4. Notice of Financial Incentive
5. Privacy Policy

Notice At Collection (CPRA Additions)

1. The purposes for which categories of both sensitive personal information and personal information are collected or used.
2. Whether collected information is sold or shared.
3. The length of time the business intends to retain each category of personal information, or where this is impossible, the criteria used to determine such period.
4. The CPRA codifies the obligation for businesses to establish clear data destruction policies and to discontinue the practice of retaining data indefinitely.
5. Notice of collection should mirror the means through which a business collects the information itself.

Notice At Collection (cont.)

Restrictions:

1. The CPRA adopts an explicit, overarching purpose limitation obligation on covered businesses. With its amendment to the CCPA, the CPRA requires that a business' collection, use, retention, and sharing of a consumer's personal information be ***“reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.”***
2. A business shall not collect categories of personal information other than those disclosed.
3. If the business provides no notice at collection, it shall not collect personal information.

Notice At Collection (cont.)

Businesses That Do Not Collect Information Directly:

- No Notice at Collection Required.
- **BUT:** Before a business can sell a consumer's personal information, it must:
 - Contact the consumer directly to provide notice of the sale and the right to opt out

OR

- Contact the source of the information to:
 1. Confirm the source provided a notice at collection AND
 2. Obtain a signed attestation from the source describing how the source gave notice at collection and include an example of the notice.

Notice Of Right To Opt Out Of Sale and Sharing Of Personal Information

Where To Provide The Notice:

Pursuant to CPRA Section 1798.135(a)(1) and (2), businesses are required to:

- Recognize “opt-out preference signal[s]” that are sent with the consumer’s consent pursuant to a technical specification that is to be created by the California Privacy Protection Agency.
- The CPRA allows the business to forgo providing these links separately and instead choose to provide a single link that enables the consumer to both limit the use and disclosure of sensitive personal information and opt out of the sale and sharing of personal information.
- ***Consent obtained through **dark patterns** does not constitute consent. CPRA defines a **dark pattern** as “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation.”

The CPRA also permits a business to forgo providing the links if they instead choose to allow consumers to opt out by sending an opt-out preference signal via “platform, technology, or mechanism.”

Businesses that substantially interact with consumers offline shall also provide the notice by an offline method.

Notice Of Right To Opt Out Of Sale and Sharing Of Personal Information (cont.)

Content of the Notice:

1. A description of the consumer's right to opt out of the sale or sharing of their personal information.
 - a) The term "sharing" is defined as the practice of providing information for the purposes of "cross-context behavioral advertising."
2. Webform by which the consumer can submit their request to opt-out online; or, if the business does not operate a website, the offline method by which the consumer can submit their request; and instructions for any other method by which the consumer may submit an opt-out request.
3. Any proof required when a consumer uses an authorized agent to exercise their right to opt out.
4. A link to or web address of the business's privacy policy.

Notice Of Right To Opt Out Of Sale and Sharing Of Personal Information (cont.)

Exemptions:

1. A business does not need to provide the notice of right to opt out of sale or sharing of personal information if:
 - a) It does not, and will not, sell or share personal information collected during the time period during which the notice of right to opt-out is not posted AND
 - b) It states in its privacy policy that it does not, and will not, sell or share personal information.

Notice of Right to Limit Use of Sensitive Personal Information

Provide a link on homepage titled, “Limit the Use of My Sensitive Personal Information,” which enables consumers to exercise their right.

Notice Of Financial Incentive

Non-Discrimination Rule:

- A financial incentive or price/service difference is discriminatory and prohibited if the business treats a consumer differently *because* the consumers exercised a right conferred by the CCPA.
- However, a business may offer a price/service difference if it is “reasonably related” to the value of the consumer’s data.

Content of the Notice:

- Succinct summary of the financial incentive or price/service difference offered.
- Description of the material terms of the financial incentive or price/service difference, including categories of personal information implicated by the financial incentive or price/service difference.
- How consumer can opt in to the financial incentive or price/service difference.
- Notification of the consumer’s right to withdraw from the financial incentive at any time and how the consumer can exercise that right.
- Explanation of why the financial incentive or price/service difference is permitted under the CCPA, including:
 - Good-faith estimate of the value of the consumer’s data that forms the basis for the offering.
 - Description of the method the business used to calculate the value of the consumer’s data.

Valuation of Consumer Data:

- A business offering a financial incentive or price or service difference shall use and document a reasonable and good faith method for calculating the value of the consumer’s data.

Our privacy policy has changed. Press 'I Agree,' because what are you really going to do about it?



Privacy Policy

Disclose information that is collected from consumers

- List categories of personal information business has collected about consumers in past 12 months, and for each category, provide:
 - Sources from which that information was collected
 - Business or commercial purposes for which information was collected
 - Categories of Third Parties with whom the business shares personal information

Disclose whether collected information is sold or shared

- State whether or not the business has disclosed, shared, or sold any personal information to Third Parties for business or commercial purpose in the past 12 months.
- List categories of personal information, if any, business has disclosed or sold to Third Parties for business or commercial purpose in the past 12 months.
- State whether the business sells personal information of minors under 16 years of age without affirmative authorization.

Inform consumers of CCPA/CPRA rights (including new/modified rights)

- Explain that the consumer has a right to request deletion of personal information collected or maintained by the business.

Inform consumers length of time for which information is kept

- The length of time you intend to retain each category of personal information or sensitive personal information you are collecting from the consumer, OR (if this is not possible)
- The criteria you use to determine how long you will retain each category of personal information or sensitive personal information you are collecting from the consumer.

Describe how consumers may exercise their rights

- Provide instructions for submitting a verifiable consumer request to delete and provide links to an online request form or portal for making the request.
- Describe the process the business will use to verify the consumer request, including any information the consumer must provide.

Privacy Policy

“Contact For More Information”

- Provide consumers with a contact for questions or concerns about the privacy policy and practices using a method reflecting how the business primarily interacts with consumers.

Date Privacy Policy Was Last Updated

Metrics Required For Businesses With Personal Information For More Than 10 Million Consumers

Responses to Consumer Requests

Methods of Submission for Requests to Know

1. A business shall provide two (2) or more designated methods for submitting consumer requests including at a minimum:
 - a. A Toll-Free Telephone Number
 - b. If the business operates a website, an interactive webform accessible through the website or mobile application
2. However, if a business operates “exclusively online” and has “a direct relationship” with the consumer from whom it collects information to “only ... provide an email address for submitting requests.”
3. If a consumer submits a request in a manner that is not one of the designated methods or is insufficient in some manner, the business shall either:
 - a. Treat the request as if it had been submitted properly OR
 - b. Provide the consumer with specific directions on how to submit the request properly.

Timing For Responses to Requests to Know and Requests to Delete

1. Confirm receipt of request **within ten (10) days** and provide information about how the business will process the request. The information should describe the verification process and when the consumer should expect a response.
2. Response to request **within 45 days** (starting from time request is received and regardless of time required to verify the request).
3. If necessary, an **additional 45 days** may be taken but the business must provide the consumer with notice and an explanation of the need for additional time.
4. A business shall not at any time disclose: Social Security Number, Driver’s License Number, Government issued identification number, Financial account number, Health insurance or medical identification number, Account password, Security questions and answers.

Responses to Consumer Requests (cont.)

Guidance for responding to Requests to Opt Out:

Business shall respond to Opt-Out requests **within 15 days** from the date the request is received.

Business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the request that the consumer has exercised their right to opt-out and instruct them not to further sell the information.

- Business must notify the consumer when this has been completed.

Opt-out request need not be verifiable. However, if a business has a good-faith, reasonable belief that request is fraudulent it may deny the request and explain why it believes the request is fraudulent.

If a business collects personal information online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, as a valid request submitted for that browser or device or customer.

Responses to Consumer Requests (cont.)

Guidance for Responding to Consumers' Request to Limit Use and Disclosure of Sensitive Personal Information:

Sensitive Personal Information that is not collected or processed for the purpose of inferring a consumer's characteristics is not subject to this right to limit its use or disclosure.

If a consumer requests that a business limits the use of their sensitive personal information, the CPRA prohibits the business from using the sensitive personal information, except for the following permitted purposes:

1. To perform services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business; and
2. Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes;
3. To undertake activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

Verifying Consumer Requests

CPRA maintains the verification process identified in the CCPA.

1. In verifying the consumer's identity, the business should:
 - a) Match identifying information provided by the consumer to personal information of the consumer already maintained by the business or use a third-party identity verification service that complies with the statute.
 - b) Avoid collecting sensitive personal information.
 - c) Avoid requesting additional information from the consumer.
 - d) The more sensitive the data or greater the risk of harm or fraud, the more stringent the verification process should be.
2. If there is no reasonable method by which a business can verify the identity of the consumer to the required degree of certainty, it shall inform the consumer and, if true for all consumers, shall so state in its privacy policy, along with an explanation of why it has no reasonable method for verifying the identity of requestors.

Special Rules for Minors

Businesses must notify minors if they intend to sell or share user data for behavioral advertising purposes.

Opt-in consent required for sale or sharing of personal information of consumers 16 or under:

- Between 13-16 – opt in consent from consumer
- Under 13 – opt in consent from parent/guardian

After a consumer under 16 years of age has declined to provide their consent to sell or share their personal information, a business must either wait for another 12 months or wait until the consumer turns 16 before requesting their opt-in consent again.

Statutory Exemptions

CCPA/CPRA shall not restrict a business's ability to:

1. Comply with federal, state, or local laws.
2. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
3. Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
4. Exercise or defend legal claims.
5. Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.
6. Collect information in connection with commercial conduct takes place wholly outside of California.

Statutory Exemptions (cont.)

CCPA shall not apply to:

1. Medical information governed by or collected by providers of health care, covered entities under Confidentiality of Medical Information Act (**CMIA**) or Health Insurance Portability and Accountability Act (**HIPAA**)
2. Information collected as part of certain clinical trials
3. Sale of personal info to/from a consumer reporting agency for use in a consumer reports governed by Fair Credit Reporting Act (**FCRA**)
4. Information collected, processed, sold, disclosed under Gramm Leach Bliley Act (**GLBA**)

Employee Privacy Rights

1. The CPRA extends the CCPA's employee and business-to-business (B2B) exemption to January 1, 2023, allowing two years for the California Legislature to address employee and B2B privacy questions in a separate bill.
2. Employees will still need to be notified at or before the point of collection of any of their personal information and purposes for collection.

Handling Employee Data

1

Review your agreements with third-party recipients of personal information of employees.

2

Implement data subject request protocols and tighten up record retention and data deletion protocols for employee information/records.

3

Consider whether and the extent to which you process “sensitive personal information” of employees, including if you use employee monitoring software, and address related CCPA requirements.

4

Update privacy policy and privacy notices to reflect how you process employee/HR data.

Miscellaneous Regulations

Training/Recordkeeping

- All individuals responsible for handling consumer inquiries about the business's privacy practices or CPRA compliance shall be informed of all requirements in the CPRA and how to direct consumers to exercise those rights.
- **A business shall maintain records of consumer requests and the business's response for at least 24 months.**
 - Consumer request information may not be used for any other purpose.
 - Aside from this information, businesses are not required to retain personal information solely for the purpose of fulfilling consumer requests.

Penalties/Remedies

California AG Enforcement Action

- \$2,500 for unintentional violation
 - 30-day option to cure
- \$7,500 for intentional violation
- Penalties paid into State AG Consumer Privacy Fund
- “Actual knowledge” a consumer is under 16 is not required.

Civil Private Right of Action

- Limited to data breach of narrower personal information (as defined in data breach statute – SSN, credit card info, health/medical info, email address in combination with a password or security question that would permit access to an email account)
 - Duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information
- Statutory Damages of \$100-\$750 per incident per consumer
- OR Actual Damages, whichever is greater

California Privacy Protection Agency (CPPA)

CPRA established California Privacy Protection Agency (CPPA):

- On July 1, 2021 the CPRA transferred rulemaking authority from the California Attorney General to the California Privacy Protection Agency.
- The CPPA was created “to implement and enforce” the CCPA and the CPRA (when it becomes operative).
- The CPPA will be the first privacy agency in the United States devoted solely to consumer data privacy and will have a broad mandate to investigate possible violations of the CPRA, enforce the CPRA through administrative action, and promulgate rules.

Requires a new rulemaking on cybersecurity and privacy:

- The CPPA shall issue regulations requiring businesses “whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security” to (1) perform a cybersecurity audit on an annual basis and (2) submit a risk assessment to the CPPA with respect to their processing of PI.

CPRA Comparison: Virginia Data Privacy Rights Act and Colorado Privacy Rights Act (Consumer Rights)

Consumer Right	CPRA	VCDPA	CPA
Right to access	✓	✓	✓
Right to confirm personal data is being processed	✓	✓	✓
Right to data portability	✓	✓	✓
Right to delete	✓	✓	✓
Right to correct	✓	✓	✓
Notice requirements	✓	✓	✓
Right to opt out of sales	✓	✓	✓
Right to opt out of targeted advertising (CO and VA and “cross context behavioral advertising”)	✓	✓	✓
Right to object to or opt-out of automated decision-making	✓	✓	✓
Opt-in or opt-out for processing of “sensitive” personal data? (“Sensitive” is defined differently under CPRA, VCDPA and CPA.)	Opt-out	Opt-in	Opt-in
Right to non-discrimination	Yes	Limited	Limited
Limited Implied Limited Purpose/use/retention limitations	✓	✓	✓
Applies to both consumers and in HR and B2B contracts	✓	✗	✗
Privacy and security impact assessments sometimes required	✓	✓	✓
Obligation to maintain reasonable security	✓	✓	✓

CPRA Comparison: Virginia Consumer Data Protection Act (VCDPA) and Colorado Privacy Rights Act

Business Obligations	CPRA	VCDPA	CPA
Data Protection Assessment	✓	✓	✓
Privacy Notice <u>at Collection</u>	✓	✗	✓
Written Contracts with Subcontractors, Third Parties, and Service Providers	✓	✓	✓
Data Minimization	✓	✓	✓
Data Security Practices	✓	✓	✓

Enforcement	CPRA	VCDPA	CPA
Data Privacy Protection Agency	✓	✗	✗
Penalties	✓	✓	✓
Private Rights of Action	✓	✗	✗
Data Minimization	✓	✓	✓
Data Security Practices	✓	✓	✓

Illinois Biometric Privacy Act (BIPA)

BIPA imposes requirements on businesses that collect or otherwise obtain biometric information, including fingerprints, retina scans and facial geometry scans (which could include identifying individuals through photographs).

Among other requirements, businesses must receive written consent from individuals before obtaining their biometric data, and they must disclose their policies for usage and retention.

Though Illinois was the first state to pass a law specifically regulating biometric data usage, other states are currently considering the issue, and Washington and Texas have already passed similar legislation.

Additional Biometric Laws

Washington

- Prohibits any company or individual from entering biometric data “in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose.” The law does not create a private right of action. The state attorney general has the enforcement rights.

Texas

- Provides that a “person may not capture a biometric identifier” without a prior consent, may not sell biometric data without consent or unless allowed by law, must use reasonable care in storing it, and “shall destroy the biometric identifier within a reasonable time.” Although it imposes a steep civil penalty of “\$25,000 for each violation,” there is no private right of action, unlike with BIPA. Rather, the state attorney general has the enforcement rights.

Colorado

- Requires opt in consent for processing of sensitive data. The statute defines “sensitive data” to mean “(a) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; (b) genetic or **biometric data** that may be processed for the purpose of uniquely identifying an individual; or (c) personal data from a known child.” The law does not create a private right of action. The state attorney general has the enforcement rights.

Virginia

- Requires opt in consent for processing of sensitive data. Sensitive data is described as **biometric data**, data collected from a known child, geolocation data, and “[p]ersonal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.” The law does not create a private right of action. The state attorney general has the enforcement rights.

Snapshot of Global Privacy Law Developments

In the **European Union**, the General Data Protection Regulation (GDPR) has been in force since May 2018. In summer 2021, the European Commission published new Standard Contractual Clauses for transfers of personal data from the European Union to “third countries” (a third country is a country other than the EU member states and the three additional EEA countries (Norway, Iceland, and Liechtenstein).)

In August 2021, **China** finalized its Personal Information Protection Law (PIPL), which will enter into force on November 1, 2021. PIPL consolidates and clarifies requirements regarding use of the personal information of Chinese residents.

Brazil's General Data Protection Law (LGPD) has been in force for a year, although the penalties provided by the law did not become enforceable until August 2021. This is Brazil's first comprehensive data protection regulation and is similar to the EU's GDPR.

India is currently voting on a Personal Data Protection Plan, a revamp of its 2000 law that looks closely at the GDPR for updates and clarifications.

Japan's Diet approved amendments to its Act on the Protection of Personal Information which will go into effect sometime within the first quarter of 2022. Under the amendments, the following personal data can no longer be provided to third parties based on the opt-out scheme: (1) personal data collected by deceit or other improper means; and (2) personal data received by a person from another person based on an opt-out scheme of that other person.

The **United Arab Emirates** (UAE) issued its first federal data protection law in 2021 alongside a law establishing the new UAE Data Office. The issuance of the Data Protection Law follows a trend of new data protection laws in the Middle East, including a data protection law in **Saudi Arabia** that will come into force on March 23, 2022.

South Korea has privacy standards on par with GDPR. South Korea's Personal Information Protection Act has been in effect since September of 2011 and from the outset has included many GDPR-like provisions, including requirements for gaining consent, the scope of applicable data, appointment of a Chief Privacy Officer, and limitation and justification of data retention periods.

Thailand's Personal Data Protection Act was supposed to come into full force on May 27, 2020, however a royal decree extended the grace period by one year. The law came into effect in 2021. The PDPA is similar to GDPR in a number of ways, including the broad definition of personal data, the requirement to establish a legal basis for collection and use of personal data, extraterritorial applicability, and penalties.

In 2018, **Chile's** Constitution was amended to include data privacy as a human right. Since then, numerous bills have been introduced to update the country's data privacy law, *Ley 19,628*, in order to guarantee legal protections that reflect the amendment.

Key Questions/Action Items For Businesses Regarding Preparedness

- **How, where, what personal information is collected/maintained in your business?**
 - Better data mapping/inventories needed to:
 - Make required disclosures
 - Respond to data access/deletion requests
 - May require working with vendors/service providers and may require additional fees
 - Data minimization (**consider what personal information is really needed, only collect what is needed, rethink what is collected**)

Key Questions/Action Items For Businesses Regarding Preparedness (cont.)

- **Do you “sell” or “share” data as defined by the CPRA (and/or do you want/need to)?**
 - If so, action items regarding disclosures and processes for response
 - Paid vs free services based on value of data
 - **If you want to avoid selling, what changes are needed to businesses’ processes?**

Key Questions/Action Items For Businesses Regarding Preparedness (cont.)

- Address vendor issues. **Are your vendors “service providers,” “contractors” or “third parties”?**
 - Consider necessary adjustments to vendor contracts with specified elements
 1. Personal information disclosed pursuant to written contract.
 2. Contract prohibits receiving entity from collecting, retaining, using, disclosing personal information for any purpose other than for the specific purpose of performing services specified in the contract or for a commercial purpose other than providing the services in the contract.
 3. Business must provide notice that info being used/shared.
 4. Includes certification made by entity receiving information that the person understands the restrictions and will comply with them.

Key Questions/Action Items For Businesses Regarding Preparedness (cont.)

- Prepare required notices/privacy policy
- Processes/infrastructure in place for handling and responding to consumer requests
- Prepare process for verifying consumers
- Prepare templates for generic/individualized responses
- Training for employees responding to consumer requests
- Data breach response plans/protocols up to date
- Cybersecurity insurance

Thank you for attending

Please direct any questions to Scott Hall and Mari Clifford.



Scott C. Hall

Partner

shall@coblentzlaw.com



Mari S. Clifford

Associate

mclifford@coblentzlaw.com