California Consumers Privacy Act(CCPA)/California Privacy Rights Act (CPRA)

Presented by

Vijaya Rajeswari Veldurthy

Senior Manager Data Privacy and Information Security

Trianz Digital Consulting Pvt Ltd

Table of Contents

California Consumers Privacy Act

The CCPA is a privacy law enacted in 2018 by the state of California to regulate the way businesses all over the world can collect, use and share the personal information of California residents. Irrespective of where you are located or operate, if you have consumers in California, Need to comply with CCPA

CCPA stands for the California Consumer Privacy Act of 2018. It has been effective from January 1, 2020, and is the first law of its kind in the United States

Note: Qualifying companies that might collect or use data about California residents, directly or through a partner, regardless of the company's location, must adhere to these guidelines.

About California Consumers Privacy Act

The CCPA was passed by the state legislature and signed by Governor Brown on June 28, 2018; it became effective on January 1, 2020

The CCPA applies to for-profit businesses that do business in California and meet any of the following:

- ✓Have a gross annual revenue of over $25 million;
- ✓Buy, sell, or share the personal information of 50,000 or more California residents, households, or devices; or
- ✓Derive 50% or more of their annual revenue from selling California residents' personal information.

Exemptions

- Personal Health Information
- Financial information

A big area of the CCPA exemption is the personal health information (PHI) that is gathered. Rather than the data being treated with the CCPA guidelines in mind, it is expected for PHI to adhere to the Health Insurance Portability and Accountability Act, otherwise known as HIPAA If the business collecting the data is related to clinical trials, then it must adhere to the "Common Rule".

As for the information that is gathered by financial institutions, the institutions follow the California Financial Information Privacy act or the Gramm-Leach-Bliley Act depending on the situation.

About CPRA- California Privacy Rights Act

The CPRA came into force on January 1, 2023, amending parts of the CCPA, which has been in effect since January 1, 2020.

The CPRA, which stands for **California Privacy Rights Act**, is an amended version of the CCPA that will make many changes to it.

Compared to its predecessor, this act is more small-business friendly. However, it will also:

- ✓ Grant consumers more rights
- ✓ Establish an agency to implement and enforce the CPRA
- ✓ Place new requirements on organizations

CPRA enforcement is from July 1, 2023.

CPRA's Legal Threshold

CPRA Legal Threshold

The CPRA introduced a new legal threshold that now applies to the CCPA, so your business falls under the jurisdiction of both laws if you do business in California and meet any **one** of the following:

- Earned $25 million in gross annual revenue as of January 1 from the previous calendar year
- Annually buys, sells, or shares the personal information of 100,000 or more California consumers or households

Derived 50% or more of your gross annual revenue from the selling or **sharing** of personal information

Personal data from the following people are now **exempt from CPRA provisions**:

- ❑ People taking part in clinical trials or biomedical research
- ❑ Healthcare providers, including medical data that is protected by the Confidentiality of Medical Information Act.

Personal Information as per CCPA

According to CCPA 1798.140(o)(1-2), "Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" is classified as personal information.
Personal information can be classified into the following categories:
Personal information like your
a)Name
b) social security number
c) email,
d) product purchase history,
e) websites you've visited,
f) geolocation data,
g) and even biometric data such as fingerprints may be collected. .

Personal Information as per CCPA

Categories of personal data											
Internal	**Description**	**Financial**	**Description**	**Historical**	**Description**	**External**	**Description**	**Social**	**Description**	**Tracking**	**Description**
Authenticating	Authentication Information belonging to the person(Ex: Passwords)	Account	A Person's financial account(Ex:Bank Account/credit card number)	Life Events	History of events that might have influneced the person's life(Ex:Wars)	Behavioral	A Person's online/offline behavior(Ex: Call Logs,attitudes etc)	Communciation	Any communication a person involved(Ex:Recordings of phone calls, emails etc)	Contact	Ways to contact a person(Ex:Email/Phone number)
Knowledge & Belief	What a person Knows or believes(Ex:Thoughts and Religious Beliefs)	Credit	A Person's financial credit & Reputation(Ex:Credit Records, credit capacity)			Demographic	A Person's charateristics(Ex:Age, Income,Geographic,physical traits)	Criminal	A person's criminal activity(Ex:charges, convictions)	Device	Devices that a person Uses(ex: IP Address, MAC Address)
Preferences	A Persons Preference's or interests(Ex: Likes/dislikes)	Ownership	Items a person owns/rents/etc.(Ex:Houses, cars,etc.)			Ethnicity	A person's ethinic origins(Ex: Race, Language,dialects)	Family	A person's family & relationships(Ex:Family structure and marriage history)	Location	A Person's physical location(Ex: Country, GPS Coordinates)
		Transactional	Income & Spending of a person(Ex: Purchase, Sales, Loans)			Identifying	Unique Information that Identifies a person(Ex:Biometric data,Govt issued ID)	Professional	Educational or professional career(Ex:Employment salary, certifications)		
						Medical & Health	Health Status & Medical conditions of a person(Ex:Overall Health,Family Health history)	Public	A person's public life(Ex:General reputation, marital status,political affiliations)		
						Physical Charateristics	A person's physical traits(Ex: Intentions, opinions etc)	Social Network	Friends or social connections of a person(Ex: Friends,connections,associations)		
						Sexual	A person's sexual life & preferences(Ex: Geneder Identity, Preferences)				

Sensitive Personal Information as per CPRA

Sensitive personal information is a new category of personal data defined by the CPRA and includes any of the following details:

1. Driving license numbers
2. Social Security Numbers (SSN)
3. State ID numbers
4. Union membership
5. Passport numbers
6. User credentials such as usernames and passwords
7. Biometric data and genetics
8. Ethnic or racial origins
9. Precise geolocations
10. Religious or philosophical beliefs
11. Information about a consumer's sexual orientation, sex life, or health
12. Contents of a consumer's text, mail, and email

Businesses now must put a "Do not Sell my Personal Information" link on their website that's easy for users to find so they can follow through on this new privacy right.

For e.g. California Privacy Statement – Infosys

Do Not Sell My Personal Information (accenture.com)

CCPA/ CPRA Consumer Rights

The consumer rights granted to Californians under the CCPA (CPRA) are:

- The right to **access** the personal information that has been collected
- The right to **correct** inaccurate personal information
- The right to **know** what personal information is being collected
- The right to **opt out** of sharing, processing and selling of information
- The right to **opt out** of automated decision-making technology
- The right of **opting in for minors**
- The right of **data portability**
- The right to **limit** the use and disclosure of sensitive personal information
- The right to **non-discrimination and non-retaliation**
- The right to request **deletion of personal data from the business that collected it and anyone who it was shared with**

Annotated Text of the CPRA with CCPA Changes | CPRA Resource Center (caprivacy.org)

Right to Access

Here's an example from Cancer Research UK. It may be a charity, but it's an example of a very **clear and concise access clause**

- The right to access allows residents of California to have access to the personal data that businesses collect on them. This means that residents of the state can request a copy of the specific personal information a business holds on them.

Typical example

Right to access your personal information

You have a right to request access to the personal data that we hold about you. You also have the right to request a copy of the information we hold about you, and we will provide you with this unless legal exceptions apply.

If you want to access your information, send a description of the information you want to see by post to Supporter Services, Cancer Research UK, PO Box 1561, Oxford, OX4 9GZ or by email to supporter.services@cancer.org.uk

Cancer Research UK's clause tells people that:

- They have a right to access the information held on them
- They can ask for a copy of the personal data stored on them
- There are at least two ways the individual can contact the company to access the data

Right to Correct Inaccurate Personal Information(new)

Consumers in California have the right to request that businesses correct any of their personal information that's inaccurate.

After receiving and verifying the authenticity of a correction request, businesses must make a reasonable effort to make the necessary corrections in accordance with regulations

Here's how San Diego-based commercial and residential moving company Corovan addresses the right to correct inaccurate information in its Privacy Policy, along with some other rights:

Right to Know What Personal Information is Collected

Essentially, consumers have a right to know:
•What **categories of personal information** you plan on collecting from them
•Why the collection is **necessary**
•Who you intend to **share the personal information with**, and **why**
•How they can opt out of **anything other than essential data collection** (that includes, for example, collecting personal data to complete a transaction and arrange goods delivery)

•Here's how OpenAI addresses the right to know in its Privacy Policy:

To the extent provided for by law and subject to applicable exceptions, California residents have the following privacy rights in relation to their Personal Information:

- The right to know information about our processing of your Personal Information, including the specific pieces of Personal Information that we have collected from you;

It's important to note that consumers should be told about these rights **before the information is collected**. It's also worth noting that the consumer **must be re-informed if you plan on changing the amount of data you collect or if you want to change who you're sharing it with**.
The best practice way to satisfy the right to know is by **having and displaying Privacy Policy**.

Wipro -We use cookies on our website to provide you with a more personalized digital experience. To learn more about how we use cookies and how you can change your cookie settings, please refer to our Privacy Statement and Cookie Classification

Right to Opt Out of Sharing, Processing and Selling(new)

Under the CCPA (CPRA), every consumer has the **right to object to you selling their data to any third party, for any purpose**. Moreover, if a consumer tells you that you can't sell their data, you can't ask them for their consent again for at **least 12 months from the day they give you their objection**.

The CCPA (CPRA) requires the displaying of a Do Not Sell My Personal Information link, for e.g.:

For e.g. California Privacy Statement – Infosys
Do Not Sell My Personal Information (accenture.com)

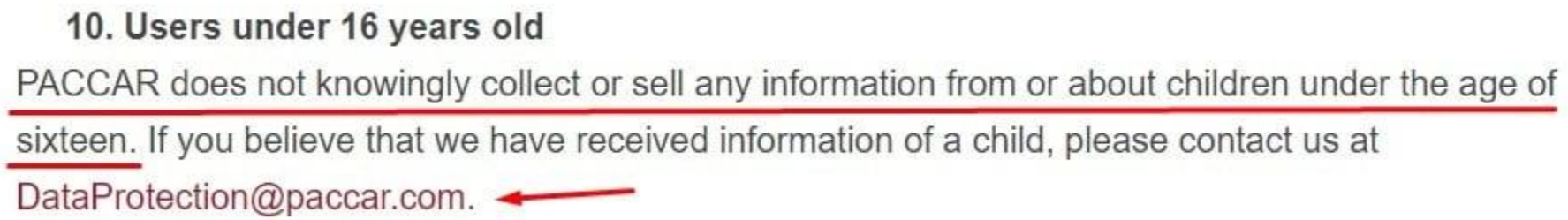
Right to Opt Out of Automated Decision-Making Technologies(new)

The CCPA (CPRA) allows consumers to opt out of the use of automated decision-making, profiling and other similar technologies.
Automated decision-making and profiling are generally defined as processes that evaluate personal aspects of a natural person and **predict future behavior**.
The types of information analyzed during the automated decision-making and profiling processes can include work, health, finance, and personal preference data to name just a few.

Automated individual decision-making, including profiling. You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects on you, except as allowed under applicable data protection laws.

Right to Opt in for Minors

Because children are particularly vulnerable, they're granted a number of age-specific rights under the CCPA (CPRA).
For example, businesses are only permitted to sell personal information collected from a child known be younger than 16 if they get authorization first. This affirmative authorization can be given by the child and is referred to as the right to opt in for minors.
On the other hand, for children younger than 13, authorization can only be granted by a parent or legal guardian.

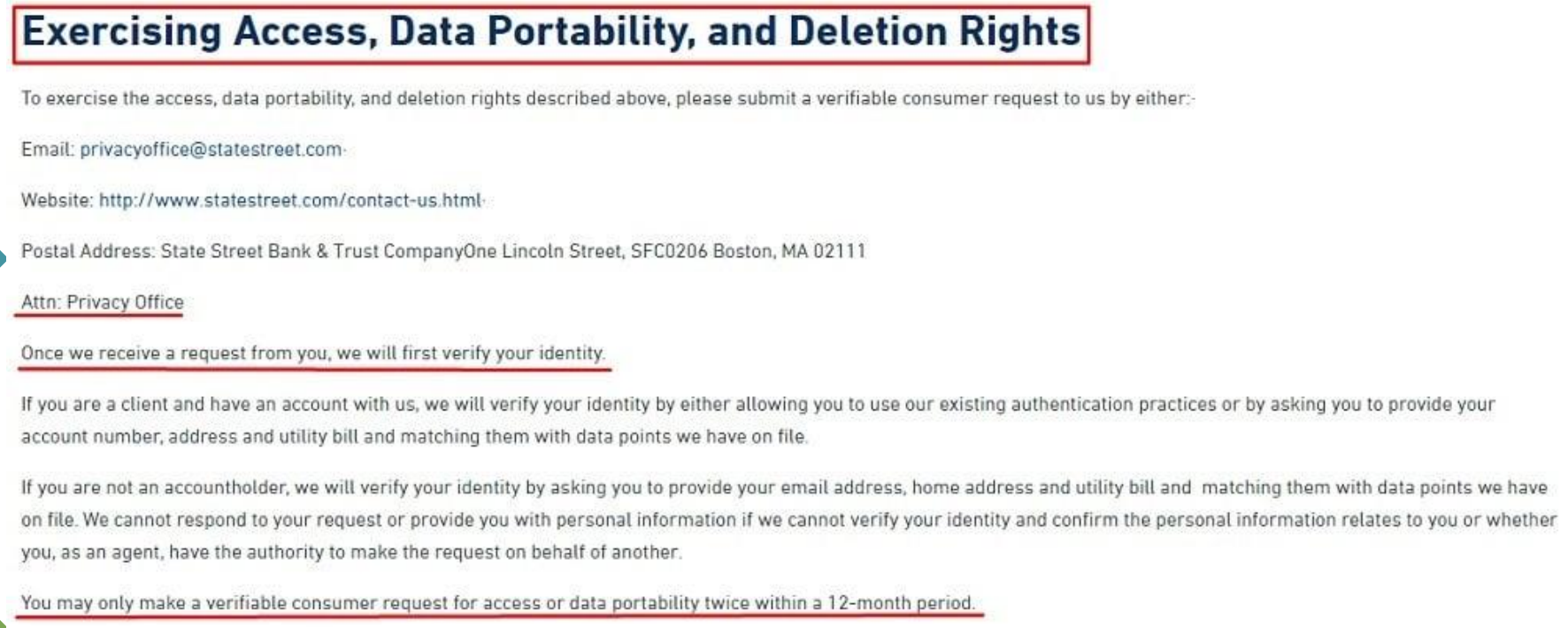


10. Users under 16 years old

PACCAR does not knowingly collect or sell any information from or about children under the age of sixteen. If you believe that we have received information of a child, please contact us at DataProtection@paccar.com.

Right to Data Portability

Under the CCPA (CPRA), consumers enjoy the right to data portability. This means that upon request, the collector must provide their data in an easily readable and commonly used format so that they can transfer or migrate it to another entity.
If they'd rather not do it themselves, consumers in California can also exercise their right to portability by requesting that a business transit some or all of their data to another entity for them.



Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by either:

Email: privacyoffice@statestreet.com

Website: http://www.statestreet.com/contact-us.html

Postal Address: State Street Bank & Trust CompanyOne Lincoln Street, SFC0206 Boston, MA 02111

Attn: Privacy Office

Once we receive a request from you, we will first verify your identity.

If you are a client and have an account with us, we will verify your identity by either allowing you to use our existing authentication practices or by asking you to provide your account number, address and utility bill and matching them with data points we have on file.

If you are not an accountholder, we will verify your identity by asking you to provide your email address, home address and utility bill and matching them with data points we have on file. We cannot respond to your request or provide you with personal information if we cannot verify your identity and confirm the personal information relates to you or whether you, as an agent, have the authority to make the request on behalf of another.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period.

Right to Limit the Use and Disclosure of Sensitive Personal Information(new)

When defining sensitive personal information, the CCPA (CPRA) includes more than a dozen data points including:

- Religious beliefs
- Sexual orientation
- Political leanings
- Health and medical information
- Geographic location

Under the CRPA amendments, Californians are able to request that a business only use their sensitive personal information when it's necessary to deliver goods or provide services.

The CPRA also introduced the requirement of an additional link on each company's homepage with the heading, *Limit the Use of My Sensitive Personal Information*.

Here's how Lynx displays a link in its website footer for more information about how a user can limit the use of sensitive personal information:

Right to Non-Discrimination and Non-Retaliation

When it comes to the collection of personal data, Californians have the right to non-discrimination, non-retaliation, and equality. In other words, businesses can't discriminate or retaliate against a consumer just because he or she refused to consent (opted out) to having personal data collected.
Here's how Inland Kenworth notes that it doesn't discriminate against customers who exercise their rights:

- **The right not to be discriminated against.** You have the right not to be discriminated against for exercising any of Your consumer's rights, including by:
  - Denying goods or services to You
  - Charging different prices or rates for goods or services, including the use of discounts or other benefits or imposing penalties
  - Providing a different level or quality of goods or services to You
  - Suggesting that You will receive a different price or rate for goods or services or a different level or quality of goods or services

Right to Request Deletion

Right to Request Deletion
If you're a business owner or data collector, it's important to know that consumers can request that you **delete their information at any time**.
To make this as easy as possible and avoid non-compliance issues down the road, it makes sense to inform them how they can initiate the process and what to expect every step of the way.
Businesses are generally required to make a good faith effort to comply with customer deletion requests, but in the following instances you may not be required to do so:
•You can't verify who sent the request
•Complying with the request may create a **security issue**
•Deletion would make difficult or impossible to complete a transaction, **initiate a recall**, or deliver a product or service
•You're currently complying with other legal obligations that take precedence
•The customer is requesting the deletion of information that the CCPA (CPRA) specifically exempts

SeaWorld addresses the right to deletion in its Privacy Policy as follows:

3. ***Deletion Request Rights***. You have the right to request that we delete any of your personal information or sensitive personal information that we collected from you and retained, subject to certain exceptions. Once we receive and verify your request (please see Subsection ***Exercising Access, Data Portability, Correction, and Deletion Rights*** below for more information), we will delete (and direct our service providers to delete) your personal information or sensitive personal information from our records, unless an exception applies. In responding to your request, we will inform you whether or not we have complied with the request, and, if we have not complied, provide you with an explanation as to why.

Responsibilities of Businesses

(1) Businesses should specifically and clearly inform consumers about how they collect and use personal information and how they can exercise their rights and choice.
(2) Businesses should only collect consumers' personal information for specific, explicit, and legitimate disclosed purposes, and should not further collect, use, or disclose consumers' personal information for reasons incompatible with those purposes.
(3) Businesses should collect consumers' personal information only to the extent that it is relevant and limited to what is necessary in relation to the purposes for which it is being collected, used, and shared.
(4) Businesses should provide consumers or their authorized agents with easily accessible means to allow consumers and their children to obtain their personal information, to delete it, or correct it, and to opt-out of its sale and the sharing across business platforms, services, businesses and devices, and to limit the use of their sensitive personal information.
(5) Businesses should not penalize consumers for exercising these rights.
(6) Businesses should take reasonable precautions to protect consumers' personal information from a security breach.
(7) Businesses should be held accountable when they violate consumers' privacy rights, and the penalties should be higher when the violation affects children.

Privacy Breach and Penalties

CCPA/CPRA sets out penalties for non-compliance.

The California Attorney General is authorized to take action against those who breach the CCPA.

The maximum civil penalty for an unintentional CCPA violation is **$2,500 per breach.**

For intentional violations, the maximum fine is **$7,500 per breach**.

violations that relate to the data of minors are tripled (**to $7,500 per violation).**

One of the most significant changes that the CPRA introduces is the establishment of the California Privacy Protection Agency (CPPA).

The CPRA will be enforced by the California Privacy Protection Agency. The agency will create a range of guidelines, addressing what is CCPA compliance, its specific requirements, and how measures will change under the CPRA.

What CCPA and CPRA Incident Response Guidelines Entail

CCPA and CPRA require businesses to implement and maintain “reasonable security procedures.” As a result, the responsibility falls on organizations to proactively protect any data they hold from being destroyed, modified, or falling into unauthorized hands.

If an organization fails to do so, they must issue a notification in compliance with the regulations’ guidelines.

Breach Response Guidelines

Who to Contact

•Any California resident who was affected by any data breach
•The state Attorney General if a single event impacts more than 500 California residents (in consultation with CPPA)

When to Make Contact

•“Without unreasonable delay” once the breach is discovered
•One exception is cases where disclosing information can hinder a law enforcement investigation

Privacy Notification of Data Breach

The notification must be written in plain language, be titled "Notice of Data Breach," and include:

- Name and contact information of the reporting organization
- Overview of what happened
- Details on the types of personal information included in the breach
- Timing information (date, estimated date, or a date range for when the breach occurred)
- Telephone numbers and addresses of major credit reporting agencies if the breach exposed social security numbers, driver's license information, or California identification card numbers
- *(Optional)* What the business has done to protect individuals affected by the breach
- *(Optional)* Advice on what affected individuals can do to protect themselves

Exemptions

Exemptions

- Organizations that fall under HIPAA's security and privacy rules.
- Financial Institutions that fall under the California Financial Information Privacy Act.
- Healthcare providers regulated by the Confidentiality of Medical Information Act.etc

6 Types of Events That Can Trigger Notification Under CCPA and CPRA

Ransomware

A ransomware attack occurs when malware steals digital information, and the attacker asks for money in exchange for releasing the data. Even if the data gets recovered, it is still exposed.

Data Theft

CCPA and CPRA treat any kind of data theft as a breach. One example is exfiltration, which is when a hacker accesses data and transfers it to their own servers or devices for ongoing access.

Improperly Sold Data

Selling individuals' personal data when they've opted out of this qualifies as a breach under CCPA and CPRA, regardless of whether it was a company effort or a rogue employee.

Mistakenly Exposed Data

Mistakenly exposing personal information, for instance by sending it to the wrong person or sharing sensitive data over an insecure channel can trigger an incident or breach response situation.

Mistakenly Updated or Deleted Data

Incorrectly updating or mistakenly deleting data, even if it was an honest mistake or an incompetent employee, requires notification under CCPA and CPRA.

Stolen or Lost Physical Records

Physical data records that become lost, get stolen, or are damaged in any way (if they are the sole copy) count as a data breach since they can then fall into the wrong hands.

Enforcement

One of the most significant changes that the CPRA introduces is the establishment of the California Privacy Protection Agency (CPPA).

The CPRA will be enforced by the **California Privacy Protection Agency**. The agency will create a range of guidelines, addressing what is CCPA compliance, its specific requirements, and how measures will change under the CPRA.

The amount of the potential administrative fine is the same as under the CCPA. In assessing fines, the agency will distinguish between two kinds of violations:

- **Unintentional violations** – When a company falls out of compliance by accident or mistake, it may incur CPRA fines up to $2,500 per violation.
- **Intentional violations** – In instances where companies intentionally mismanage consumer data, fines of up to $7,500 per violation may apply.

However, a key difference under the CPRA is that fines increase to $7,500 for each violation of CPRA involving the personal information of consumers under the age of 16.

California: CPPA proposes revisions to CCPA Regulations and introduces draft insurance regulations

On November 30, 2023, the California Privacy Protection Agency (CPPA) published proposed revisions to the California Consumer Privacy Act Regulations (CCPA Regulations) and draft Insurance Regulations, for discussion during the board meeting scheduled for December 8, 2023

•add the personal information of consumers less than 16 years of age as a new category of sensitive personal information;
•adjust monetary thresholds, including:
- increasing, from January 1, 2023, the threshold indicated within the definition of 'business' under the CCPA to $27,975,000; and
- increasing civil penalty amounts to not more than $2,797.50 for each violation or $8,392.50 for each intentional violation and violations involving the personal information of consumers whom the violator has actual knowledge are under 16 years of age;

•clarify that third parties are persons to whom the personal information is sold or shared, not disclosed 'for a business purpose;'
•add further examples that demonstrate the symmetry principle when obtaining consumer consent; and
•add language to reflect the businesses' new requirement to display the status of the consumer's choice in relation to opt-out preference signals, which was removed from a previous draft of the CCPA Regulations.

California: CPPA proposes revisions to CCPA Regulations and introduces draft insurance regulations

On November 30, 2023, the California Privacy Protection Agency (CPPA) published proposed revisions to the California Consumer Privacy Act Regulations (CCPA Regulations) and draft Insurance Regulations, for discussion during the board meeting scheduled for December 8, 2023

What do the draft Insurance Regulations seek to introduce?

The draft Insurance Regulations would clarify that insurance companies that meet the definition of 'business' under the CCPA shall comply with the CCPA with regard to any personal information that they collect, use, process, or retain for purposes not subject to the Insurance Code.

Privacy Framework

Privacy Information Management System Framework comprises Set of Policies, Procedures, Guidelines and Checklist

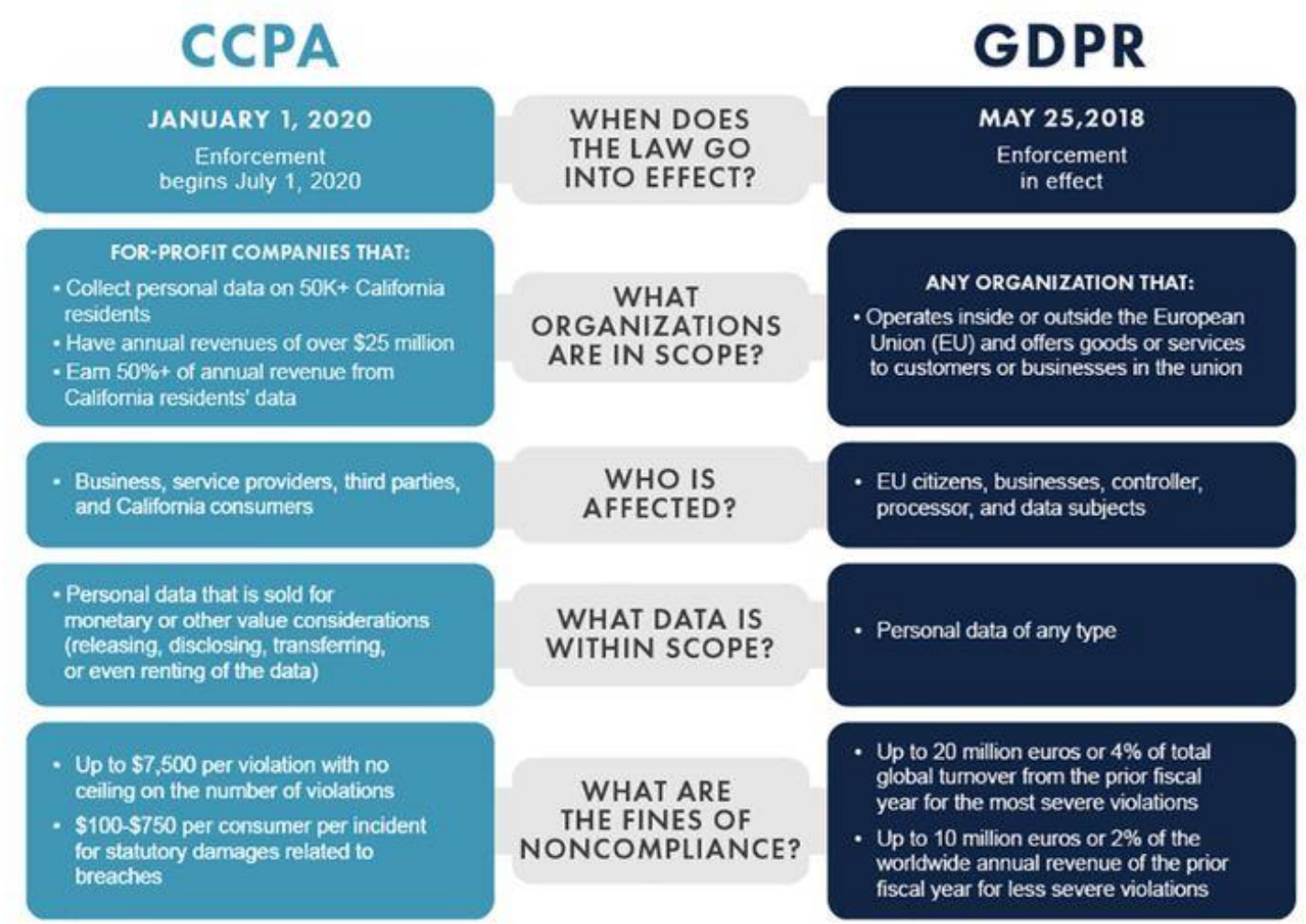
Privacy Governance comprises the Privacy Team lead by DPO

Privacy Policies include – Data Protection Policy, Data Retention and Disposal Policy etc

Privacy Procedures include – Data Subjects rights procedure, Data Retention and Disposal Procedure, Consent Procedure, Consent Withdrawal Procedure, Privacy by design procedure, Breach notification Procedure, Privacy Impact Assessment Procedure

Templates include to ensure all the DSAR (Data subject Access Requests), Breach Notification Template, Privacy Impact Assessment Template

CCPA vs GDPR


CCPA
GDPR
JANUARY 1, 2020
Enforcement begins July 1, 2020
WHEN DOES THE LAW GO INTO EFFECT?
MAY 25,2018
Enforcement in effect
FOR-PROFIT COMPANIES THAT:
• Collect personal data on 50K+ California residents
• Have annual revenues of over $25 million
• Earn 50%+ of annual revenue from California residents' data
WHAT ORGANIZATIONS ARE IN SCOPE?
ANY ORGANIZATION THAT:
• Operates inside or outside the European Union (EU) and offers goods or services to customers or businesses in the union
• Business, service providers, third parties, and California consumers
WHO IS AFFECTED?
• EU citizens, businesses, controller, processor, and data subjects
• Personal data that is sold for monetary or other value considerations (releasing, disclosing, transferring, or even renting of the data)
WHAT DATA IS WITHIN SCOPE?
• Personal data of any type
• Up to $7,500 per violation with no ceiling on the number of violations
• $100-$750 per consumer per incident for statutory damages related to breaches
WHAT ARE THE FINES OF NONCOMPLIANCE?
• Up to 20 million euros or 4% of total global turnover from the prior fiscal year for the most severe violations
• Up to 10 million euros or 2% of the worldwide annual revenue of the prior fiscal year for less severe violations

Other Sector Specific Laws

- **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)** regulates health information privacy rights. Individuals have the rights to access the personal information in their health records, ask to change wrong, missing, or incomplete information, know who the information is shared with, and limit sharing of it. HIPAA covers health care providers, hospitals and clinics, insurers, and certain third party businesses, like pharmacies. It does not cover health care apps and wearable devices like Fitbit.
- **The Gramm-Leach-Bliley Act (GLBA),** enacted in 1999, is primarily a piece of financial services reform legislation. Buried within it, though, are rules that address consumer financial privacy. The GLBA requires financial institutions to disclose to customers, in a “clear and conspicuous” privacy notice, the types of “nonpublic personal information" (NPI) it collects about them, how it’s used, and who it’s shared with. They must also provide an opt-out mechanism to customers who don’t want their information shared with unaffiliated companies. Therein lies a major loophole: among affiliates in the same “corporate family,” customer NPI rights don’t apply.
- **The Fair Credit Reporting Act (FCRA)** of 1970 predates the Privacy Act and deals with the personal information contained in consumer credit reports. Under the FCRA, consumers have the right to know what information is in their credit file, dispute any errors in it, and whether it has been used against them in an “adverse action” (such as being denied employment). Entities that compile credit reports, send information contained in credit reports, and use credit reports are subject to the FCRA.
- **The Children’s Online Privacy Protection Act (COPPA)** regulates personal information collected from children younger than thirteen. It imposes requirements on commercial websites and online service providers that collect, disclose, or use personal information from twelve and under. COPPA compliance is enforced by the Federal Trade Commission (FTC). Violations can result in a fine. Several social media and tech companies have violated the COPPA, including TikTok ($5.7 million fine) and YouTube ($170 million fine).

Other States and Privacy Laws

“

•**The California Consumer Privacy Act (CCPA)** cemented California as one of the top states for consumer protection by extending consumer rights to the personal data sphere. Ironically, California Democrats could be an obstacle to nationwide legislation if a privacy bill does not offer protections that are at least equal to those in California. Former House Speaker Nancy Pelosi and other California officials were credited with shelving the ADPPA on these grounds.
•**The California Privacy Rights Act (CPRA)**, which takes effect January 1, 2023 and amends the CCPA, is California’s second legislative foray into data privacy. It gives Californians new data rights, changes the criteria for covered businesses, and introduces data minimization principles, and creates a new state regulatory agency. A recent California court order has delayed CPRA enforcement until March 29, 2024.
•**The Colorado Privacy Act (CPA)** enhances consumer privacy protection by giving Colorado residents five major rights and imposing duties on covered entities. Based in large part on the failed Washington Privacy Act, it adopts the controller-processor approach found in the EU’s GDPR. The law went into effect July 1, 2023.
•**The Connecticut Data Privacy Act (CTDPA)** made Connecticut the fifth state to adopt data privacy legislation. While the CTDPA takes many of its cues from similar state laws, most notably the CPA, it also has a few unique provisions, such as not requiring consumer opt-outs to be authenticated. The CTDPA took effect on July 1, 2023.
•**The Virginia Consumer Data Protection Act (VCDPA)** was the second broad data privacy bill to win state approval. The VCDPA, a middle ground between pro-consumer and pro-business interests, moved quickly through the legislature and passed by a large margin. The law became effective January 1, 2023.
•**The Utah Consumer Privacy Act (UCPA)** is seen by privacy experts as more business-friendly than comparable state laws. As the first “red” state to pass a law of this kind, Utah shows that data privacy is a bipartisan issue. The UCPA approved by the state legislature in just 5 working days, goes into effect December 23, 2022.
•**Iowa SF 262** was signed into law on March 29, 2023, making Iowa the sixth state to pass comprehensive privacy legislation. It takes a similar approach to other state privacy laws and has been compared most closely to Utah’s for its business-friendly provisions. The law will go into effect on January 1, 2025.
•**The Indiana Consumer Data Protection Act (ICDPA)** was enacted on May 1, 2023. The transparency and disclosure obligations that the Indiana Consumer Data Protection Act places on covered entities are similar to those in Colorado, Connecticut, and Virginia, but Indiana is giving companies a 2.5-year runway to prepare for a January 1, 2026 effective date.
•**The Tennessee Information Protection Act (TIPA)** was the third state data privacy law in six weeks—and the 8th overall—to gain a governor’s signature after it passed unanimously through both houses of the state legislature. Like Iowa, Utah, and Virginia laws, the TIPA takes a more business-friendly approach. It goes into effect July 1, 2025.
•**The Montana Consumer Privacy Act (MCDPA)** joined the ranks of state privacy law on May 19, 2023. Scheduled to take effect on October 1, 2024, the MCDPA closely resembles the Connecticut Data Privacy Act in several key aspects, including permitting consumers to opt out of the processing or sale of personal data for targeted advertisements.
•**The Texas Data Privacy and Security Act (TDPSA)** made Texas the tenth state to pass a data privacy bill, and the fifth to enact or pass one in a seven week span. Passed on May 29 and signed by Governor Abbott on June 18, the Texas law borrows from Virginia’s but throws in a few twists, such as a unique three-factor coverage threshold standard. The TDPSA will take effect on July 1, 2024.
•**The Oregon Consumer Privacy Act (OCPA)** was the eleventh U.S. legislation (the sixth in 2023), to pass. Husch Blackwell calls it “one of the strongest” such laws passed so far. Senate Bill 619 is largely similar to laws in other states but is noteworthy for not providing a broad exemption to non-profits or entities regulated by HIPAA. Once signed into law, the OCPA will take effect on July 1, 2024.

American Data Privacy Protection Act

The American Data Privacy Protection Act (ADPPA) was introduced on June 21, 2022, and has enjoyed more bipartisan support than any other federal data privacy proposal to date[12]. It was approved by the Committee on Energy and Commerce on July 20, 2022, with a 53-2 vote[3]. However, it failed to advance to the House or Senate floors in the last Congress[3]. It is unclear whether the ADPPA has sufficient support to become law, as it reportedly lacks key support in the Senate[4].

What if ADPPA passes

The ADPPA would also preempt recently enacted state privacy laws, including California, Virginia, Colorado, Utah, and Connecticut 2.

2. The Act has several main principles: data minimization, individual ownership, and private right of action . The burden of evaluating each organization's programs would fall to the organization 1.

3. Data collectors would have to minimize the data they collected down to that which was "necessary, proportionate, and limited to" their purpose, whether administering a product or communicating 1.

4. Individuals would have the right under ADPPA to know how their personal data was to be used and which third parties would have received it. They would have had the right to correct and download their user data 1.

5. Organizations would have had up to 90 days to process these requests, depending on the organization's size 1.

6. Individuals would also have had the right to take legal action against organizations in violation of the Act for four years after its execution after first giving their state Attorney General and Federal Trade Commission 60 days' notice to respond 1.

7/ Designated "large data holders" would have been subject to additional controls

Thank you