GDPR vs U.S. State Privacy Laws

The table below sets out the key requirements of U.S. state privacy laws in California, Virginia, Colorado, Connecticut, and Utah, and provides a comparison against similar concepts under the EU General Data Protection Regulation (GDPR). The table does not cover every aspect of these laws but is intended to provide a digest of U.S. state privacy requirements against the GDPR. Please note that the information contained in this document is current as of February 2023. Additional requirements are likely to be introduced into U.S. state laws, including by way of implementing regulations and rules that are not covered below.

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Name of legislation	California Consumer Privacy Act (**CCPA**), as amended by the California Privacy Rights Act (**CPRA**)	Virginia Consumer Data Protection Act **(VDPA)**	Colorado Privacy Act (**CPA**)	Connecticut Data Privacy Act (**CDPA**)	Utah Consumer Privacy Act (**UCPA**)	General Data Protection Regulation (**GDPR**)
Regulations	CCPA Regulations	N/A	CPA Regulations	N/A	N/A	N/A[1]
Effective date	January 1, 2023[2]	January 1, 2023	July 1, 2023	July 1, 2023	December 31, 2023	May 25, 2018
Scope						
Material scope	Applies to a business that: • does business in CA, • collects consumers' personal information, AND • determines why and how personal information is processed	Applies to a person that: • conducts business in VA, OR • produces products or services that are targeted to VA consumers	Applies to a controller that: • conducts business in CO, OR • produces or delivers products or services intentionally targeted to CO consumers	Applies to a person that: • conducts business in CT, OR • produces products or services that are targeted to CT consumers	Applies to a controller or processor that: • conducts business in UT, OR • produces products or services that are targeted to UT consumers	Applies to a controller or processor that: • is established in the EU, OR • offers goods or services in the EU, OR • monitors behaviour of EU data subjects

[1] While the GDPR does not have or require implementing regulations, EU data protection authorities issue regulatory guidance and the European Data Protection Board (EDPB) issues opinions and recommendations on certain topics. Additionally, while the GDPR has direct effect across the EU, most Member States have enacted domestic legislation that incorporates and/or supplements the GDPR under national law.
[2] Enforcement of the amendments under the CPRA begins on July 1, 2023.

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Threshold criteria[3]	• $25m gross annual revenue, OR • buys, sells, or shares personal information of ≥100,000 CA consumers or households, OR • derives ≥50% of revenue from sale or sharing of personal information of CA consumers	• controls or processes personal data of ≥100,000 VA consumers, OR • controls or processes personal data of ≥25,000 VA consumers AND derives >50% gross revenue from sale of personal data	• controls or processes personal data of ≥100,000 CO consumers, OR • controls or processes personal data of ≥25,000 CO consumers AND derives revenue or receives a discount on the price of goods or services from sale of personal data	• controls or processes personal data of ≥100,000 CT consumers, OR • controls or processes personal data of ≥25,000 CT consumers AND derives >25% gross revenue from sale of personal data	• ≥$25m annual gross revenue AND controls or processes personal data of ≥100,000 UT consumers, OR • controls or processes personal data of ≥25,000 UT consumers AND derives ≥50% of gross revenue from sale of personal data	N/A
Covered entities	Applies to **businesses**, **service providers** and **contractors**[4]	Applies to **controllers** and **processors**	Applies to **controllers** and **processors**	Applies to **controllers** and **processors**	Applies to **controllers** and **processors**	Applies to **controllers** and **processors**[5]
Notable exemptions[6]						
Non-profit organisations	✓	✓	N/A[7]	✓	✓	N/A
Publicly-available information	✓[8]	✓	✓	✓	✓	N/A

[3] In additional to material scope, certain threshold criteria must be met for U.S. state laws to apply.
[4] Under the CCPA, a business is a legal entity that *"(a) collects consumers' personal information on its own or by others on its behalf, (b) alone or jointly with others determines the purposes and means of the processing, (c) does business in California"* and satisfies at least one of the three threshold criteria. A service provider is a person that "*processes personal information on behalf of a business and that receives from or on behalf of the business a consumer's personal information for a business purpose*." A contractor is a person *"to whom the business makes available a consumer's personal information for a business purpose*."
[5] Under the GDPR, a controller is an entity "*which, alone or jointly with others, determines the purposes and means of the processing of personal data*" and a processor is an entity "*which processes personal data on behalf of the controller*". The VDPA, CPA, CDPA and UCPA have similar definitions.
[6] This section sets out certain types of organisations and data that are exempt from the applicable requirements.
[7] Unlike other U.S. state privacy laws, the CPA does not exempt non-profit organisations.
[8] The CPRA expanded the exemption for publicly available information to include both information that is lawfully made available from federal, state, or local government records and true "public" information that is made available to the general public by the consumer or from widely distributed media.

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Employee data within employment context	N/A[9]	✓[10]	✓[11]	✓[12]	✓[13]	N/A
Personal data within B2B context	N/A[14]	✓[15]	✓[16]	✓[17]	✓[18]	N/A
Covered entities, business associates & protected health information subject to Health Insurance Portability and Accountability Act (HIPAA)	✓	✓	✓	✓	✓	N/A
Financial institutions & data subject to Gramm-Leach-Bliley Act (GLBA)	✓	✓	✓	✓	✓	N/A
Student data subject to Family Educational Rights and Privacy Act (FERPA)	N/A	✓	✓	✓	✓	N/A
Consumer reporting information subject to Fair Consumer Reporting Act (FCRA)	✓	✓	✓	✓	✓	N/A

[9] The CCPA exemption for HR data expired on January 1, 2023.
[10] The VDPA includes an exemption for personal data processed in the course of an individual applying to, employed by, or acting as agent of the controller.
[11] The CPA definition of "consumer" excludes individuals acting in an employment context or as a job applicant.
[12] The CDPA includes an exemption for personal data processed in the course of an individual applying to, employed by, or acting as agent of the controller.
[13] The UDPA includes an exemption for personal data processed in the course of an individual applying to, employed by, or acting as agent of the controller.
[14] The CCPA exemption for B2B data expired on January 1, 2023.
[15] The VDPA definition of "consumer" excludes individuals acting in a commercial context.
[16] The CPA definition of "consumer" excludes individuals acting in a commercial context.
[17] The CDPA definition of "consumer" excludes individuals acting in a commercial context as employees, owners, directors, officers or contractors where their communications or transactions occur within context of their role.
[18] The UCPA definition of "consumer" excludes individuals acting in a commercial context.

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Personal data						
Definition of personal data (or equivalent term)	**Personal information** is any 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	**Personal data** is any information that is linked or reasonably linkable to an identified or identifiable natural person	**Personal data** is any information that is linked or reasonably linkable to an identified or identifiable individual	**Personal data** is any information that is linked or reasonably linkable to an identified or identifiable individual	**Personal data** is any information that is linked or reasonably linkable to an identified or identifiable individual	**Personal data** is any information relating to an identified or identifiable natural person
Data outside scope of personal data (or equivalent term)	**De-identified data** is information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer pro vided that the business takes certain steps **Aggregate consumer information** is information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device	**De-identified data** is data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person provided that the controller takes certain steps	**De-identified data** is data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual provided that the controller takes certain steps	**De-identified data** is data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual provided that the controller takes certain steps	**De-identified data** is data that cannot reasonably be linked to an identified or identifiable individual provided that the controller takes certain steps **Aggregate data** is information that relates to a group or category of consumers, from which individual consumer identities have been removed and that is not linked or reasonably linkable to any consumer	**Anonymous data** is information which does not relate to an identified or identifiable natural personal of personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Categories of sensitive data[19]						
Health data	✓	✓	✓	✓	✓	✓
Genetic data	✓	✓	✓	✓	✓	✓
Biometric data	✓	✓	✓	✓	✓	✓
Race or ethnic origin	✓	✓	✓	✓	✓	✓
Religious beliefs	✓	✓	✓	✓	✓	✓
Philosophical beliefs	✓	N/A	N/A	N/A	N/A	✓
Political opinions	N/A	N/A	N/A	N/A	N/A	✓
Sex life or sexual orientation	✓	✓	✓	✓	✓	✓
Citizenship or immigration status	N/A	✓	✓	✓	✓	N/A
Trade union membership	✓	N/A	N/A	N/A	N/A	✓
Precise geolocation	✓	✓	N/A	✓	✓	N/A
SSN, driver's license, state ID or passport no.	✓	N/A	N/A	N/A	N/A	N/A
Account log-in, financial account, debit or credit card number in combination with access code, password or credentials	✓	N/A	N/A	N/A	N/A	N/A
Mail, email or SMS content	✓	N/A	N/A	N/A	N/A	N/A[20]
Children's data	N/A	✓	✓	✓	N/A	N/A[21]

[19] The processing of sensitive data may give rise to additional requirements, as set out below.
[20] Although not considered sensitive data under the GDPR, mail, email and SMS content is potentially regulated by the ePrivacy Directive.
[21] Although not considered sensitive data under the GDPR, there are specific requirements that apply to children's data under the GDPR as set out below.

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Special requirements for sensitive data						
Requirement	Consumers have the right to **limit the use and disclosure of sensitive information** to the extent necessary to provide goods or services reasonably expected by the average consumer Sensitive information that is collected or processed without the purpose of inferring sensitive characteristics about the consumer is not subject to this requirement and can be treated as non-sensitive information	Consumers must **consent** to processing of sensitive data	Consumers must **consent** to processing of sensitive data	Consumers must **consent** to processing of sensitive data	Consumers have the right to be notified about the processing of sensitive data and **opt out**	Sensitive data may only be processed under certain **conditions**, including if (a) based on the data subject's explicit consent, (b) required under employment, social security and social protection law, (c) necessary for the data subject's vital interests, (d) necessary for legitimate activities carried out by a foundation, association or other non-profit, (e) manifestly made public by the data subject, and (f) necessary for legal claims.
Data protection rights						
Right to confirm processing	✓	✓	✓	✓	✓	✓
Right of access	✓	✓	✓	✓	✓	✓
Right to correct	✓	✓	✓	✓	N/A	✓
Right to delete	✓	✓	✓	✓	✓	✓
Right to data portability	✓ Access right includes right to obtain copy in structured, commonly used, machine-readable format that may be	✓ Access right includes right to obtain copy in portable and readily-usable format that allows the consumer to	✓ Access right includes right to obtain copy in portable and readily-usable format that allows the consumer to	✓ Access right includes right to obtain copy in portable and readily-usable format that allows the consumer to	✓ Access right includes right to obtain copy in portable and readily-usable format that allows the consumer to	✓

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
	transmitted to another entity at the consumer's request without hindrance	transmit the data to another controller without hindrance	transmit the data to another entity without hindrance	transmit the data to another controller without hindrance	transmit the data to another controller without impediment	
Right to object	N/A	N/A	N/A	N/A	N/A	✓[22]
Right to restrict processing	N/A	N/A	N/A	N/A	N/A	✓[23]
Right to opt-out of sale	✓ A **sale** is disclosing, making available, or otherwise communicating personal information to another business or third party for monetary or other valuable consideration	✓ A **sale** is the exchange of personal data for monetary consideration	✓ A **sale** is the exchange of personal data for monetary or other valuable consideration	✓ A **sale** is the exchange of personal data for monetary or other valuable consideration	✓ A **sale** is the exchange of personal data for monetary consideration	N/A
Right to opt-out from sharing or targeted advertising	✓ **Sharing** means disclosing, making available or otherwise communicating personal information to a third party for **cross-context behavioral advertising**, which means targeting advertising based on the consumer's personal information obtained across businesses and distinctly-branded websites, applications or services	✓ **Targeted advertising** means displaying advertisements that are selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests	✓ **Targeted advertising** means displaying advertisements that are selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict the consumer's preferences or interests	✓ **Targeted advertising** means displaying advertisements that are selected based on personal data obtained or inferred from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests	✓ **Targeted advertising** means displaying advertisements that are selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests	N/A[24]

[22] This right applies where the controller is relying on legitimate interests as its legal basis for processing.
[23] This rights applies in limited circumstances, for example where the data subject disputes the accuracy of their data or the lawfulness of processing.
[24] Although the GDPR does not include a specific right to opt out from targeted advertising, this type of processing is potentially regulated by the ePrivacy Directive.

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Right to limit use of sensitive data	✓ Consumers have the right to limit the use and disclosure of sensitive data to the extent necessary to provide goods or services reasonably expected by the average consumer	N/A	N/A	N/A	✓ Consumers have the right to be notified about the processing of sensitive data and opt out	N/A[25]
Rights regarding automated decision-making	✓ Consumers have the right to opt out of automated decision making[26]	✓ Consumers have the right to opt out of profiling that involves decisions producing legal or similarly significant effects	✓ Consumers have the right to opt out of profiling that involves decisions producing legal or similarly significant effects	✓ Consumers have the right to opt out of profiling that involves decisions producing legal or similarly significant effects	N/A	✓ Automated decision-making is only permitted if it is (a) necessary to perform a contract between the data controller and the data subject, (b) based on the data subject's explicit consent, or (c) authorised by law. Data subjects have the right to contest automated decisions and obtain human intervention
Right to appeal decisions	N/A If the business denies a consumer request, it must inform the reasons for not taking action and any rights the consumer may have to appeal the decision	✓ Controllers must establish a process for consumers to appeal the controller's refusal to act on a request within a reasonable time	✓ Controllers must establish a process for consumers to appeal the controller's refusal to take action on a request within a reasonable time	✓ Controllers must establish a process for consumers to appeal the controller's refusal to take action on a request within a reasonable time	N/A If the business denies a consumer request, it must inform the reasons for not taking action	N/A[27]

[25] Although the GDPR does not include a right to limit the use of sensitive data, certain conditions apply to the processing of sensitive data as set out above.

[26] The nature and scope of this right will be set out in CCPA Regulations to be issued by the California Privacy Protection Agency.

[27] The VDPA, CPA and CDPA include specific rights for consumers to appeal against the controller's decision regarding how they have handled a rights request. No such right exists under the GDPR, however data subjects always have the right to complain to EU data protection authorities.

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Deadline for response	**10 business days to confirm receipt** **45 calendar sdays to respond** (+45 days extension) **15 business days for opt-out requests**	**45 days** (+45 days extension)	**45 days** (+45 days extension)	**45 days** (+45 days extension)	**45 days** (+45 days extension)	**1 month** (+2 months extension)
Key obligations						
Data minimisation	✓ A business's collection of personal information must be **reasonably necessary and proportionate** to achieve the purposes for which it was collected	✓ A controller must limit the collection of personal data to what is **adequate, relevant, and reasonably necessary** in relation to the purposes for which such data is processed, as disclosed to the consumer	✓ A controller's collection of personal data must be **adequate, relevant, and limited to what is reasonably necessary** in relation to the specified purposes for which the data are processed	✓ A controller must limit the collection of personal data to what is **adequate, relevant, and reasonably necessary** in relation to the purposes for which such data is processed, as disclosed to the consumer	N/A	✓ Personal data must be **adequate, relevant and limited to what is necessary** in relation to the purposes for which it is processed
Purpose limitation	✓ A business's use of personal information must be **reasonably necessary and proportionate** to achieve the purposes for which the information was collected, or for another disclosed purpose that is compatible with the context in which the	✓ Controllers must not process personal data for purposes that are **neither reasonably necessary to nor compatible with** the disclosed purposes for which such data is processed, as disclosed to the consumer, unless the controller obtains the consumer's **consent**	✓ Controllers must not process personal data for purposes that are **not reasonably necessary to or compatible with** the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's **consent**	✓ Controllers must not process personal data for purposes that are **neither reasonably necessary to nor compatible with** the disclosed purposes for which such data is processed, as disclosed to the consumer, unless the controller obtains the consumer's **consent**	N/A	✓ Personal data must be collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
	information was collected, and not further processed in a manner that is incompatible with those purposes					
Transparency[28]	✓ • Categories of personal information & sensitive data collected • Categories of sources • Business & commercial purposes • Confirmation whether business uses or discloses sensitive data for non-specified purposes • Categories of personal data disclosed for business & commercial purpose & third parties with whom personal information is disclosed for	✓ • Categories of personal data • Purposes for processing • Categories of personal data shared • Categories of third parties with whom personal data is shared • Categories of personal data sold or processed for targeted advertising • Explanation of rights	✓ • Categories of personal data • Purposes for processing • Categories of personal data shared • Categories of third parties with whom personal data is shared • Whether personal data is sold or processed for targeted advertising • Explanation of rights	✓ • Categories of personal data • Purposes for processing • Categories of personal data shared • Categories of third parties with whom personal data is shared • Whether personal data is sold or processed for targeted advertising • Explanation of rights	✓ • Categories of personal data • Purposes for processing • Categories of personal data shared • Categories of third parties with whom personal data is shared • Whether personal data is sold or processed for targeted advertising • Explanation of rights	✓ • Categories of personal data • Categories of sources • Purposes for processing • Legal basis for processing • Categories of personal data shared • Categories of third parties with whom personal data is shared • Explanation of rights • Data transfers • Data retention • Contact details for DPO & representative

[28] This information must be set out in the controller's (or business's) privacy notice

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
	business & commercial purpose • Confirmation whether business has actual knowledge that it sells or shares personal information • Categories of personal information sold or shared & third parties with whom personal information is sold or shared • Explanation of rights • Data retention • Summary of financial incentives • Date policy was last updated					
Fairness & non-discrimination	✓ Businesses must not **discriminate against consumers** for exercising their rights under the CCPA. Loyalty programs, rewards & discounts may be offered	✓ Controllers must not process personal data in violation of **US laws prohibiting discrimination**, or discriminate against consumers for exercising their rights under the VDPA. Loyalty programs, rewards & discounts may be offered	✓ Controllers must not process personal data in violation of **US laws prohibiting discrimination**, or change costs or availability of the service due to consumer exercising their rights under the CPA. Loyalty programs, rewards & discounts may be offered	✓ Controllers must not process personal data in violation of **US laws prohibiting discrimination**, or discriminate against consumers for exercising their rights under the CDPA. Loyalty programs, rewards & discounts may be offered	✓ Controllers must not **discriminate** against consumers for exercising their rights under the UCPA. Loyalty programs, rewards & discounts may be offered	✓ Personal data must be processed **fairly**

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Data security	✓ Businesses must implement **reasonable security procedures and practices** appropriate to the nature of the personal information to protect the information from unauthorised or illegal access, destruction, use, modification, or disclosure	✓ Controllers must establish, implement and maintain **reasonable administrative, technical and physical data security practices** to protect the confidentiality, integrity and accessibility of personal data	✓ Controllers must take **reasonable measures** to secure personal data during both storage and use from unauthorised acquisition	✓ Controllers must establish, implement and maintain **reasonable administrative, technical and physical data security practices** to protect the confidentiality, integrity and accessibility of personal data	✓ Controllers must establish, implement, and maintain **reasonable administrative, technical, and physical data security practices** designed to (a) protect the confidentiality and integrity of personal data, and (b) reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data	✓ Controllers and processors must implement **appropriate technical and organisational measures** to ensure a level of security for personal data which is commensurate to the risks involved in the processing
Special requirements for children's data	✓ Businesses must obtain **opt-in consent** to sell or share personal information of children under 16 and **parental consent** to sell or share personal information of children under 13[29]	✓ Controllers must obtain **parental consent** to process data of children under 13 in accordance with COPPA	✓ Controllers must obtain **parental consent** to process data of children under 13. However, the CPA does not apply to children's data where the data is collected, processed, and maintained in compliance with COPPA	✓ Controllers must obtain **parental consent** to process data of children under 13 in accordance with COPPA	✓ Controllers must obtain **parental consent** in compliance with COPPA when processing personal data of children under 13	✓ Controller must obtain **parental consent** if relying on consent to process data of children under 13-16[30] in relation to an offer of information society services directly to the child[31]

[29] California has also passed AB-2273, the California Age Appropriate Design Code, that resembles the UK's Age Appropriate Design Code.
[30] Member States are free to determine the age of a child for the purposes of this requirement, between the ages of 13 and 16.
[31] This requirement does not necessarily apply outside of the online services context (i.e., "information society services"). However, handling children's data more generally warrants an enhanced privacy approach under the GDPR, for example to provide "appropriate" levels of transparency. Also, note that controllers have child-specific obligations as per regulatory guidance, such as the UK's Age Appropriate Design Code or Ireland's Fundamentals for a Child-Oriented Approach to Data Processing.

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Special requirements for financial incentives	✓ Businesses must notify consumers of any **financial incentives** and may only enter a consumer into a financial incentive program if the consumer gives prior **opt-in consent**	N/A	N/A	N/A	N/A	N/A
Data protection impact assessments	✓ Businesses must conduct **risk assessments** for processing that presents a significant risk to consumers' privacy or security32	✓ Controllers must conduct **data protection assessments** for (a) sale of personal data, (b) targeted advertising, (c) profiling involving reasonably foreseeably risks, (d) processing of sensitive data, (e) other processing that presents a heightened risk of harm to consumers	✓ Controllers must conduct **data protection assessments** for (a) sale of personal data, (b) targeted advertising, (c) profiling involving reasonably foreseeably risks, (d) processing of sensitive data, (e) unfair or deceptive treatment, or unlawful disparate impact, or financial or physical injury for consumers, (f) other processing that presents a heightened risk of harm to consumers	✓ Controllers must conduct **data protection assessments** for (a) sale of personal data, (b) targeted advertising, (c) profiling involving reasonably foreseeably risks, (d) processing of sensitive data, (e) other processing that presents a heightened risk of harm to consumers	N/A	✓ Controllers must conduct **data protection impact assessments** for processing that is likely to result in a high risk to data subjects' rights and freedoms, including (a) automated decision making, (b) processing of sensitive data on a large scale, (c) systematic monitoring of a publicly accessible area on a large scale

[32] The nature and scope of this requirement will be set out in CCPA Regulations to be issued by the California Privacy Protection Agency.

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Data processing terms[33]	✓ • Description of specific business purposes • Service provider prohibited from (a) selling or sharing personal information, (b) retaining, using, or disclosing personal information for any purpose except the business purposes or outside the direct business relationship, (c) combining personal information with information received from or on behalf of another person • Service provider must provide same level of protection as required by CCPA • Business may take reasonable and appropriate steps to ensure service provider is using personal information in a manner	✓ • Description of processing • Instructions for processing • Personnel must be subject to duty of confidentiality • Processor may only engage sub-processors if bound by written contract • Processor must assist controller with security, breach notification, and data protection assessments • Processor must make available all information to demonstrate compliance and allow for audits and inspections • Processor must return or delete personal data after provision of services •	✓ • Description of processing • Instructions for processing • Personnel must be subject to duty of confidentiality • Processor may only engage sub-processors if (a) bound by written contract, and (b) controller can object • Processor must ensure appropriate level of security • Processor must make available all information to demonstrate compliance and allow for audits and inspections • Processor must return or delete personal data after provision of services •	✓ • Description of processing • Instructions for processing • Personnel must be subject to duty of confidentiality • Processor may only engage sub-processors if (a) bound by written contract, and (b) controller can object • Processor must make available all information to demonstrate compliance and allow for audits and inspections • Processor must return or delete personal data after provision of services •	✓ • Description of processing • Instructions for processing • Personnel must be subject to duty of confidentiality • Processor may only engage sub-processors if bound by written contract • Processor must assist controller with security and breach notification •	✓ • Description of processing • Processor must only act under controller's instructions • Personnel must be subject to duty of confidentiality • Personal data must be protected through appropriate security measures • Processor may only engage sub-processors if (a) sub-processor bound by written contract, (b) controller provides specific or general authorisation, (c) processor notifies controller of changes and controller can object • Processor must assist controller with data subject requests and data

[33] These terms must be entered between controllers and processors (or businesses and service providers)

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
	consistent with the business' obligations and may stop and remediate unauthorised use of personal information • Service provider must notify business if it can no longer meet its obligations under CCPA • Service provider may only engage subcontractors if bound by contract that complies with the CCPA • Service provider must assist controller with data subject requests and data protection impact assessments • Service provider must return or delete personal data after provision of services	•				protection impact assessments • Processor must make available information to demonstrate compliance, including audits and inspections • Processor must return or delete personal data after provision of services
Enforcement						
Rulemaking	**California Privacy Protection Agency**	N/A	**Colorado Attorney General**	N/A	N/A	National **data protection authorities** may issue binding codes or guidance

	California (CA)	Virginia (VA)	Colorado (CO)	Connecticut (CT)	Utah (UT)	European Union (EU)
Enforcement	California Privacy Protection Agency & California Attorney General	Virginia Attorney General	Colorado Attorney General & District Attorneys	Connecticut Attorney General	Utah Attorney General & Utah Department of Commerce	National data protection authorities
Fines	**$2,500 per violation** or **$7,500 per violation** for intentional violations & violations involving children's data	**$7,500 per violation**	**$20,000 per violation** A violation of the CPA is a deceptive trade practice under the Colorado Consumer Protection Act, which carries up to $20,000 fine per violation	**$5,000 per violation** A violation of the CDPA is considered an unfair trade practice under the Connecticut Unfair Trade Practices Act, which carries up to $5,000 fine per violation	**$7,500 per violation**	**4% global revenue** or **€20 million**, whichever is higher
Private right of action	✓ Up to **$750 per consumer per incident** or **actual damages**. Limited to security breaches involving non-encrypted and non-redacted personal information	N/A	N/A	N/A	N/A	✓ Data subjects may claim **compensation** for material and non-material damage against controllers or processors
Cure period	✓ **30 days** for consumer actions & discretionary cure period for regulatory enforcement	✓ **30 days**	✓ **60 days**[34]	✓ **60 days**[35]	✓ **30 days**	N/A

Fieldfisher (Silicon Valley) LLP – February, 2023

[34] This cure period sunsets on January 1, 2025.
[35] This cure period sunsets on January 1, 2025.