**Definition of Sale**  
(§ 6-1-1303 (23))

"Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party.  
(1) The disclosure of personal data to a processor that processes the personal data on behalf of the controller.  
(2) The disclosure of personal data to a third party for purposes of providing a product or service requested by a consumer.  
(3) The disclosure or transfer of personal data to an affiliate of the controller.  
(4) The disclosure of personal data in which the consumer intentionally made the personal data available to the general public via a channel of mass media, and did not restrict to a specific audience.  
(5) The disclosure or transfer of personal data when a consumer uses or directs a controller to disclose or intentionally discloses by using the controller to interact with a third party.  
(6) The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.  
(§ 13-61-101(23)).

**Definition or Reference to Other of Pseudonymous Data**  
- Personal information that cannot be attributed to an identifiable individual.  
- Subject to additional technical and organizational measures.  

**Enforcement and Controller Requirements**  
- Subject to additional technical and organizational measures.  

**California**  
- Yes (§ 1996.105(i)).  

**Virginia**  
- No (§ 55-1-729 (C)).

**Connecticut**  
- Yes (§ 1-1310).  
- Yes (§1-1310(c)).

**District of Columbia**  
- Yes (20 days) (§ 55-1-579(b)).  
- Yes (20 days).  
- § 55-1-579(b).  
- Yes (20 days) (§ 13-61-402 (3)).

**Georgina**  
- Yes (30 days) (§ 11(b)).

**Indiana**  
- Yes (30 days) (§ 1710.8(R)).

**Iowa**  
- Yes (30 days) (§ 7150.8(R)).  
- Yes (30 days) (§ 7150.8(R)).

**Kansas**  
- Yes (5) (§ 5).

**Kentucky**  
- Yes (5) (§ 5).

**Louisiana**  
- Yes (5) (§ 5).

**Maine**  
- Yes (5) (§ 5).

**Massachusetts**  
- Yes (5) (§ 5).

**Montana**  
- Yes (5) (§ 5).

**Nebraska**  
- Yes (5) (§ 5).

**Nevada**  
- Yes (5) (§ 5).

**New Hampshire**  
- Yes (5) (§ 5).

**New Jersey**  
- Yes (5) (§ 5).

**New Mexico**  
- Yes (5) (§ 5).

**New York**  
- Yes (5) (§ 5).

**North Carolina**  
- Yes (5) (§ 5).

**North Dakota**  
- Yes (5) (§ 5).

**Ohio**  
- Yes (5) (§ 5).

**Oklahoma**  
- Yes (5) (§ 5).

**Oregon**  
- Yes (5) (§ 5).

**Pennsylvania**  
- Yes (5) (§ 5).

**Puerto Rico**  
- Yes (5) (§ 5).

**Rhode Island**  
- Yes (5) (§ 5).

**South Carolina**  
- Yes (5) (§ 5).

**South Dakota**  
- Yes (5) (§ 5).

**Tennessee**  
- Yes (5) (§ 5).

**Texas**  
- Yes (5) (§ 5).

**Utah**  
- Yes (5) (§ 5).

**Vermont**  
- Yes (5) (§ 5).

**Virginia**  
- Yes (5) (§ 5).

**Washington**  
- Yes (5) (§ 5).

**West Virginia**  
- Yes (5) (§ 5).

**Wisconsin**  
- Yes (5) (§ 5).

**Wyoming**  
- Yes (5) (§ 5).
**Pseudonymous Data Exceptions**

- No requirement to respond to a request to delete pseudonymized data (Cal. Code Regs. tit. 10, § 995.323(i)).
- No requirement to respond to a request to provide deidentified data (Cal. Code Regs. tit. 10, § 995.323(i)).
- No requirement to respond to a request to provide pseudonymized data (Cal. Code Regs. tit. 10, § 995.323(i)).
- No requirement to respond to a request to correct pseudonymous data (Section 6-1-1303(3)).

1. The disclosure of personal data to a processor that processes the personal data on behalf of the controller.

2. The disclosure of personal data to a processor to provide a product or service requested by the consumer.

**Definitions and Exclusions**

- No requirement to respond to a request to delete deidentified data (Cal. Code Regs. tit. 11, § 999.323(i)).
- No requirement to respond to a request to provide pseudonymized data (Cal. Code Regs. tit. 11, § 999.323(i)).
- No requirement to respond to a request to provide deidentified data (Cal. Code Regs. tit. 11, § 999.323(i)).
- No requirement to respond to a request to provide pseudonymized data (Cal. Code Regs. tit. 11, § 999.323(i)).

**Sensitive Data Definition**

- "Sensitive Personal Information means (1) Personal information that reveals: (A) A consumer’s social security driver’s license, state identification card, 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; (B) A consumer’s account login, fingerprint data, biometric data based on a consumer’s face or iris or other pattern or design, or union membership; (C) The contents of a consumer’s mail, email, and text messages unless the business is the intended recipient of the communication; (D) Personal information collected and analyzed concerning a consumer’s health; (E) Personal information collected and analyzed concerning a consumer’s age; (F) Personal information collected and analyzed concerning a consumer’s sex, gender identity, or sexual orientation; (G) Personal information that is "publicly available" pursuant to paragraph (2) of subdivision (c) that shall not be considered sensitive personal information or organizational information; (H) Personal information (a) 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 processed for the purpose of uniquely identifying an individual; or (c) personal data of a known child."

See Finalized Regs. Rule 6.10 for more information on duties regarding sensitive data.

- "Sensitive data means: (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 processed for the purpose of uniquely identifying an individual; or (c) personal data of a known child."

See Finalized Regs. Rule 6.10 for more information on duties regarding sensitive data.

**Definition or References to Inferences**

- "Inference" or "inference" means the derivation of information, data, conclusions, or conclusions from fact, evidence, or another source of information or data. (§ 1798.100(a)).
- Sensitive Personal Information that is collected for the purpose of inferring characteristics about a consumer is subject to a consumer’s right to limit use and disclosure. (§ 1798.121).
- The implementation regulations also define "sensitive information" -- "Sensitive Data Definitions" or "Sensitive Data Definitions" means information maintained by a business based on Personal Data, alone or in combination with other data, which are collected from a known child, or (c) personal data of a known child."

See Finalized Regs. Rule 6.10 for more information on duties regarding sensitive data.

*"Inference" as referenced in C.R.S. 6- 1-1303(24)(a) includes Sensitive Data Definitions *While the classification information at a high level may not be considered Sensitive Data Definitions *Privacy geolocation data which is used to identify a person’s location in real time is considered Sensitive Data Definitions. Regs. (1/27 version) Rule 2.02

**Definitions or References to Inferences**

- "No requirement to respond to a request to delete identified data or pseudonymized data; or (2) collect, obtain, retain, or use any personal data; or (3) process personal data; or (4) use personal data (Chapter 7 Section 93(3) and 1752.4 (11))".

- No requirement to respond to a request to delete identified data or pseudonymized data; or (2) collect, obtain, retain, or use any personal data; or (3) process personal data; or (4) use personal data (Chapter 7 Section 93(3) and 1752.4 (11)).

- No requirement to respond to a request to delete identified data or pseudonymized data; or (2) collect, obtain, retain, or use any personal data; or (3) process personal data; or (4) use personal data (Chapter 7 Section 93(3) and 1752.4 (11)).

- No requirement to respond to a request to delete identified data or pseudonymized data; or (2) collect, obtain, retain, or use any personal data; or (3) process personal data; or (4) use personal data (Chapter 7 Section 93(3) and 1752.4 (11)).

- No requirement to respond to a request to delete identified data or pseudonymized data; or (2) collect, obtain, retain, or use any personal data; or (3) process personal data; or (4) use personal data (Chapter 7 Section 93(3) and 1752.4 (11)).
A business that collects a consumer’s personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into a contract with its service provider or contractor; that contract shall identify specific business purposes for which the service provider or contractor is processing personal information pursuant to the contract; and a service provider or contractor shall only disclose the personal information it collected for any commercial purpose or for any other than the Business Purposes specified in the contract, unless expressly permitted by the CCPA or these regulations. A processor or service provider or contractor from sharing, using, or disclosing the personal information it collects with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. 

-Require service provider or contractor to notify the business if it makes a determination that it can no longer meet obligations under the CCPA and these regulations. 
-Grant the business the right to take reasonable and appropriate steps to ensure that the processor or contractor provides the personal information that it Collects pursuant to the written contract with the business in a manner consistent with the business’s obligations under the CCPA and these regulations. 
-Require the service provider or contractor to notify the consumer if the processor or contractor does not comply with and provide the information necessary for the service provider or contractor to comply with the requirements described in paragraphs (i)(6) and (i)(7) (B) (47-18-3205(b)).

A business that collects a consumer’s personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into a contract with its service provider or contractor; that contract shall identify specific business purposes for which the service provider or contractor is processing personal information pursuant to the contract; and a service provider or contractor shall only disclose the personal information it collected for any commercial purpose or for any other than the Business Purposes specified in the contract, unless expressly permitted by the CCPA or these regulations. A processor or service provider or contractor from sharing, using, or disclosing the personal information it collects with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. 

-Require service provider or contractor to notify the business if it makes a determination that it can no longer meet obligations under the CCPA and these regulations. 
-Grant the business the right to take reasonable and appropriate steps to ensure that the processor or contractor provides the personal information that it Collects pursuant to the written contract with the business in a manner consistent with the business’s obligations under the CCPA and these regulations. 
-Require the service provider or contractor to notify the consumer if the processor or contractor does not comply with and provide the information necessary for the service provider or contractor to comply with the requirements described in paragraphs (i)(6) and (i)(7) (B) (47-18-3205(b)).
<table>
<thead>
<tr>
<th>Service Provider / Processor Obligations with Consumer Rights Flowing from Businesses / Controllers</th>
<th>California</th>
<th>Virginia</th>
<th>Colorado</th>
<th>Connecticut</th>
<th>Iowa</th>
<th>Indiana</th>
<th>Mississippi</th>
<th>Tennessee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consumer Rights</strong></td>
<td>Opt in for Sale</td>
<td>Age 13-10: opt in. (§ 798.120(d))</td>
<td>Opt in for secondary use (§ 798.120(e)) and for sensitive data (§ 798.120(f)).</td>
<td>Opt-in for “known children” (Age &lt; 13) in accordance with COPPA.</td>
<td>Opt in for sensitive data (§ 6).</td>
<td>No opt-in for sale, but requires entities to follow COPPA.</td>
<td>Required before the sale of children’s data. (Chapter 4 Section 1 (5)).</td>
<td>opt-in required before the sale of data of a known child (under 13) (§ 7(b)(o)).</td>
</tr>
<tr>
<td></td>
<td>Opt out of sale for known user</td>
<td>Yes; opt out. (§ 798.120(a))</td>
<td>Yes; opt out. (§ 798.120(a)(ii)).</td>
<td>Yes; opt-out (§ 13-61-101(14a)).</td>
<td>Yes; opt-out (§ 13-61-101(14a)).</td>
<td>Yes; opt-out (§ 4(a)(5)).</td>
<td>Yes; opt-out (§ 715D.3(i)).</td>
<td>Yes; opt-out (§ 5(1)(a)).</td>
</tr>
<tr>
<td></td>
<td>Opt out of sale for pseudonymous or inference data</td>
<td>Yes, included in right to opt out of sale (§ 798.120).</td>
<td>Yes, included in right to opt out of sale (§ 798.120(d)).</td>
<td>Pseudon. Included in right to opt out of sale. (§ 6-1-303(1)).</td>
<td>Pseudon. Included in right to opt out of sale (§ 6-1-303(1)).</td>
<td>Pseudon. Included in right to opt out of sale (§ 6-1-303(1)).</td>
<td>Yes; opt-out (Chapter 3 Section 1 (b)).</td>
<td>No, consumer rights do not apply to pseudonymous data (§ 6-1-302(1)).</td>
</tr>
<tr>
<td></td>
<td>Separate Opt Out for Targeted Advertising</td>
<td>Pseudon. Included in sale. (§ 798.120)</td>
<td>Pseudon. Included in right to opt out of sale (§ 6-1-303(1)).</td>
<td>Separate from sale. (§ 6-1-303(1)(a)(i)).</td>
<td>Separate from sale. (§ 6-1-303(1)(a)(i)).</td>
<td>Separate from sale. (§ 4(a)(5)(A)).</td>
<td>Yes – Chapter 3 Section 13(d)(A).</td>
<td>No, included in sale (§ 17-2302(a)(2)).</td>
</tr>
<tr>
<td></td>
<td>Separate Opt Out of Profiling</td>
<td>No (§ 798.140(a)(1)).</td>
<td>Yes, right to opt out of profiling separately from sale. (§ 58.1-573A(4)(B)).</td>
<td>Yes, right to opt out of profiling separately from sale. (§ 6-1-303(1)(a)(i)).</td>
<td>No. Right to opt out of profiling separately from sale (Chapter 6-1-303(1)(a)(i)).</td>
<td>Yes, right to opt out of profiling separately from sale. (§ 715D.4(i)).</td>
<td>No, No. Right to opt out of profiling separately from sale. (§ 715D.4(i)).</td>
<td>No, included in sale of personal data (§ 47-18-3201(8)(1)).</td>
</tr>
<tr>
<td></td>
<td>Opt In for Sale of Personal Information</td>
<td>Yes (§ 798.110)</td>
<td>Yes (§ 59.1-574A(5)(B)).</td>
<td>Yes (§ 6-1-308(b)(7)).</td>
<td>Yes (§ 6-1-101(23)).</td>
<td>Yes (§ 6(a)(4)).</td>
<td>No (§ 7(b)(2)).</td>
<td>Yes (§ 17-2302(a)(6)).</td>
</tr>
<tr>
<td></td>
<td>Access to Information (Specific Pieces of Information)</td>
<td>Yes (§ 798.110)</td>
<td>Yes (§ 59.1-575A(b)).</td>
<td>Yes (§ 6-1-308(b)(7)).</td>
<td>Yes (§ 6-1-101(23)).</td>
<td>Yes (§ 6(a)(4)).</td>
<td>No (§ 7(b)(2)).</td>
<td>Yes (§ 17-2302(a)(6)).</td>
</tr>
<tr>
<td></td>
<td>Access Right (Categories)</td>
<td>Yes; categories of PI; categories of sources of PI; business purpose of processing; categories of third parties PI has been disclosed to; specific pieces of PI collected. (§ 798.110)</td>
<td>No, categories required in privacy policy (§ 59.1-573C(5)).</td>
<td>No, categories required in privacy policy (§ 6-1-303(1)(a)(ii)).</td>
<td>No, categories required in privacy policy (§ 6-1-302(1)(A)).</td>
<td>No, categories required in privacy policy (§ 6-1-302(1)(A)).</td>
<td>No, categories required in privacy policy (§ 715D.4(i)).</td>
<td>No, categories required in privacy policy (§ 715D.4(i)).</td>
</tr>
<tr>
<td></td>
<td>Deletion Right</td>
<td>Yes (§ 798.105(b))</td>
<td>Yes (§ 59.1-573(3)).</td>
<td>Yes (§ 6-1-306(d)).</td>
<td>Yes (§ 6-1-306(d)).</td>
<td>Yes (§ 6-1-306(d)).</td>
<td>Yes (§ 6(a)(3)).</td>
<td>Yes, the consumer has the right to delete the personal information that they provided to the controller only. (§ 715D.3 (b)).</td>
</tr>
<tr>
<td></td>
<td>Consumer Rights</td>
<td>Yes (§ 798.120(c)).</td>
<td>Yes (§ 6-1-308(d)).</td>
<td>Yes (§ 6-1-308(d)).</td>
<td>Yes (§ 6-1-308(d)).</td>
<td>Yes (§ 6-1-308(d)).</td>
<td>Yes (§ 6(a)(3)).</td>
<td>Yes, the consumer has the right to delete the personal information that they provided to the controller only. - (§ 715D.3 )</td>
</tr>
</tbody>
</table>

**Note:** Per finalized regs as of 5/23, data rights request methods do not need to be specific to CO (§ 715D.2(c)).
<table>
<thead>
<tr>
<th>State</th>
<th>Nonretaliation Right</th>
<th>Health-related Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>California</td>
<td>Yes; additional requirements from CCPA. Business cannot &quot;harass&quot; or discriminate against an employee, applicant for employment, or independent contractor for exercising their rights under this title. Additionally, “[b]usinesses may not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, requiring the consumer to pay a higher price or rate for a good or service, or providing a different level of quality of goods or services to the consumer.” (§ 1789.120)</td>
<td>Under the definition of sensitive data, data that reveals mental or physical health diagnosis requires companies to provide consumers with notice of their ability to opt-out of its processing (§ 1789.140(i)).</td>
</tr>
<tr>
<td>Nevada</td>
<td>Yes; controller may not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, requiring the consumer to pay a higher price or rate for a good or service, or providing a different level of quality of goods or services to the consumer.” (§ 59.1-574(A)(4)).</td>
<td>Under the definition of sensitive data, information regarding an individual’s medical history, mental or physical health condition or medical treatment or diagnosis by a health care professional requires companies to provide consumers with notice of their ability to opt-out of its processing (§13-61-101(22)).</td>
</tr>
<tr>
<td>Utah</td>
<td>Yes. “A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in sections 1 to 11, inclusive, of this act, including denying goods or services, charging different prices or rates for goods or services, requiring the consumer to pay a higher price or rate for a good or service, or providing a different level of quality of goods or services to the consumer.” (§ 6(a)(7)).</td>
<td>Under the definition of sensitive data, data that is revealing a mental or physical health diagnosis requires companies to provide consumers with clear notice and an opportunity to opt out of such processing. (§715D-4(2))</td>
</tr>
<tr>
<td>Colorado</td>
<td>No right but controllers have a duty to avoid unlawful discrimination. (§ 6-1-1308 (b)).</td>
<td>Under the definition of sensitive data, data that is a mental or physical health condition or diagnosis requires companies to provide consumers with clear notice and an opportunity to opt out of such processing. (§715D-4(2))</td>
</tr>
<tr>
<td>Connecticut</td>
<td>Yes. “A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in sections 1 to 11, inclusive, of this act, including denying goods or services, charging different prices or rates for goods or services, requiring the consumer to pay a higher price or rate for a good or service, or providing a different level of quality of goods or services to the consumer.” (§ 6(a)(7)).</td>
<td>Under the definition of sensitive data, data that is a mental or physical health condition or diagnosis requires companies to provide consumers with clear notice and an opportunity to opt out of such processing. (§715D-4(2))</td>
</tr>
<tr>
<td>Indiana</td>
<td>Yes. A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against a consumer. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. (§ 6-1-1023(f)).</td>
<td>Yes -- controller may not discriminate against a consumer for exercising the rights set forth (§715D-4(2)).</td>
</tr>
<tr>
<td>Montana</td>
<td>Yes -- controller may not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods and services, or providing a different level of quality or goods or services to the consumer. (§ 715D-4(2))</td>
<td>Under the definition of sensitive data, data revealing &quot;a mental or physical health condition or diagnosis&quot; requires opt in consent. (§47-18-3201 (25)(i))</td>
</tr>
<tr>
<td>Tennessee</td>
<td>Yes -- controller may not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods and services, or providing a different level of quality of goods and services to the consumer. (§ 715D-4(2))</td>
<td>Under the definition of sensitive data, data revealing &quot;a mental or physical health condition or diagnosis&quot; requires opt in consent. (§47-18-3201 (25)(i))</td>
</tr>
</tbody>
</table>