

US State Data Broker Laws Comparison Chart

State	Definition of Data Broker ⁱ	Applicability Standard	Annual Registration Requirement	Registration Disclosure Obligations ⁱⁱ	Privacy Policy Disclosure Obligations	Creates Substantive Consumer Rights	Delete Request & Opt-out Platform (DROP)	Other Notable Provisions	Fines
California	A business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship ⁱⁱⁱ	Must qualify as a business under California Consumer Privacy Act	✓	✓	✓	✗ <i>*But creates DROP mechanism through which consumers can exercise rights</i>	✓ Data brokers must process requests starting Aug. 1, 2026	Third-party audit requirement starting July 1, 2028	\$200 per day for failing to register + \$200 per day for each deletion request not processed
Connecticut ^{iv}	Any business or, if such business is not an individual, any portion of such business that sells or licenses brokered personal data to another person	“Business” means (i) any person who regularly engages in commercial activities for purpose of generating income, (ii) any bank, Connecticut credit union, federal credit union, out-of-state bank, out-of-state trust company or out-of-state credit union, as such terms are defined in section 36a-2 of the general statutes, and (iii) any other person who controls, is controlled by or is under common control with any person described above. It does not include any body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of Connecticut	✓	✓	✓	✗ <i>*But creates DROP mechanism through which consumers can exercise rights</i>	✓ Data brokers must process requests starting Oct. 1, 2028	Third-party audit requirement starting July 1, 2031	\$200 per day, per violation
Nevada	Person whose primary business is purchasing covered information about consumers with whom person does not have direct relationship and who reside in Nevada from operators or other data brokers and	-	✗	✗	✗	✓	✗	-	\$5,000 per violation

State	Definition of Data Broker ⁱ	Applicability Standard	Annual Registration Requirement	Registration Disclosure Obligations ⁱⁱ	Privacy Policy Disclosure Obligations	Creates Substantive Consumer Rights	Delete Request & Opt-out Platform (DROP)	Other Notable Provisions	Fines
	making sales of such covered information								
Oregon	Business entity or part of business entity that collects and sells or licenses brokered personal data to another person	“Business entity” means: (i) a resident individual who regularly engages in commercial activity for the purpose of generating income; (ii) a corporation or nonprofit corporation, LLC, partnership or LLP, business trust, joint venture or other form of business organization the constituent parts of which share a common economic interest; (iii) a financial institution, as defined in ORS 706.008; or (iv) another person that controls, is controlled by or is under common control with a person described above. It does not include the state or a state agency, a local government, as defined in ORS 174.116, a public corporation or a business entity or other person during a period in which the business entity or person is acting solely on behalf of and at the direction of the state, a state agency, the local government or a public corporation.	✓	✓	✗	✗	✗	Data brokers must notify the director of data breaches within 45 days of the breach	\$500 per violation per day with \$10,000 annual cap
Texas	Business entity that collects, processes, or transfers personal data that the business entity did not collect directly from the individual linked or linkable to the data.	Law applies to data brokers that, in a 12-month period, derive: (1) more than 50% of revenue directly from processing or transferring personal data not collected by data broker directly from individuals to whom data pertains; or (2) revenue directly from processing or transferring personal data of more than 50,000 individuals not collected by data broker directly from individuals to whom data pertains	✓	✓	✗ <i>*But see “other” column</i>	✗	✗	Data brokers must post data broker notice on website Data brokers must have comprehensive information security program	\$100 daily fine + amount of unpaid registration fee with \$10,000 annual cap

State	Definition of Data Broker ⁱ	Applicability Standard	Annual Registration Requirement	Registration Disclosure Obligations ⁱⁱ	Privacy Policy Disclosure Obligations	Creates Substantive Consumer Rights	Delete Request & Opt-out Platform (DROP)	Other Notable Provisions	Fines
Vermont ^v	A business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship ^{vi}	“Business” means a commercial entity, including a sole proprietorship, partnership, corporation, association, LLC, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of Vermont, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but does not include the State of Vermont, a State agency, any political subdivision of the State, or a vendor acting solely on behalf of, and at the direction of, the State	✓	✓	✗	✗	✗	<p>Data brokers must maintain a \$20,000 bond that runs to the state for any liability arising from violations of data broker law</p> <p>Data brokers must maintain procedures requiring prospective users of brokered personal information to identify themselves, state the purposes for which information is sought, and certify that the information shall be used for no other purpose</p> <p>Data brokers must conduct due diligence on recipients of brokered personal information</p> <p>Data brokers have separate security breach notification obligations</p> <p>Data brokers must have comprehensive information security programs</p>	<p>\$200 per day for failing to register plus registration fees</p> <p>\$1,000 per day for each day data broker fails to provide all required registration information starting 30 days after discovery</p> <p>\$25,000 civil penalty plus \$1,000 per each day data broker fails to correct materially incorrect information starting 30 days after discovery</p>

State	Information Covered
California	<p>“Personal information” means 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 information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers. (B) Any personal information described in subdivision (e) of Section 1798.80. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an internet website application, or advertisement. (G) Geolocation data. (H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or employment-related information. (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99). (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. (L) Sensitive personal information.</p>
Connecticut	<p>“Brokered personal data” means one or more of the following personal data elements concerning a consumer, if categorized or organized for sale or license to a third party: (A) Name; (B) address; (C) date of birth; (D) place of birth; (E) mother’s maiden name; (F) unique biometric data (i) generated from measurement or technical analysis of a human body characteristic, including, but not limited to, a fingerprint, retina or iris image or other unique physical or digital representation of biometric data, and (ii) used by the owner or licensee of such unique biometric data to identify or authenticate the consumer; (G) name or address of a member of the consumer’s immediate family or household; (H) Social Security number or other government-issued identification number; or (I) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.</p>
Nevada	<p>“Covered information” means any one or more of the following items of personally identifiable information about a consumer collected by an operator through an Internet website or online service and maintained by the operator or a data broker in an accessible form: (1) A first and last name. (2) A home or other physical address which includes the name of a street and the name of a city or town. (3) An electronic mail address. (4) A telephone number. (5) A social security number. (6) An identifier that allows a specific person to be contacted either physically or online. (7) Any other information concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator or data broker in combination with an identifier in a form that makes the information personally identifiable.</p>
Oregon	<p>“Brokered personal data” means any of the following computerized data elements about a resident individual, if categorized or organized for sale or licensing to another person: (A) The resident individual’s name or the name of a member of the resident individual’s immediate family or household; (B) The resident individual’s address or an address for a member of the resident individual’s immediate family or household; (C) The resident individual’s date or place of birth; (D) The maiden name of the resident individual’s mother; (E) Biometric information about the resident individual; (F) The resident individual’s Social Security number or the number of any other government-issued identification for the resident individual; or (G) Other information that, alone or in combination with other information that is sold or licensed, can reasonably be associated with the resident individual.</p>
Texas	<p>“Personal data” means any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the information is used by a controller or processor in conjunction with additional information that reasonably links the information to an identified or identifiable individual. The term does not include deidentified data, employee data, or publicly available information.</p>
Vermont	<p>“Brokered personal information” means any information, including derived data and unique identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or to a device that identifies, is linked to, or is reasonably linkable to one or more identified or identifiable individuals in a household.</p>

ⁱ Each law should be checked for additional entity exemptions.

ⁱⁱ These states require data brokers to provide additional information (such as information relating to their data processing activities) to regulators when registering.

ⁱⁱⁱ Direct relationship means “that a consumer has intentionally interacted with a business for the purpose of accessing, purchasing, using, requesting, or obtaining information about the business’s products or services. A consumer does not have a “direct relationship” with a business if the purpose of their engagement is to exercise any right described under Civil Code section 1798, or for the business to verify the consumer’s identity. A business does not have a “direct relationship” with a consumer simply because it collects personal information directly from the consumer; the consumer must intend to interact with the business. A business is still a data broker and does not have a direct relationship with a consumer as to personal information it sells about the consumer that it collected outside of a “first party” interaction with the consumer, as that term is defined in California Code of Regulations, title 11, section 7001.”

^{iv} Connecticut’s data broker law is effective October 1, 2026, with data brokers required to register by January 1, 2027.

^v As amended by H.211 effective January 1, 2027.

^{vi} “Direct relationship” means that a consumer has intentionally interacted with a business for the purpose of accessing, purchasing, using, requesting, or obtaining information about the business’s products or services. A consumer does not have a direct relationship with a business if the purpose of the consumer’s engagement is to exercise a consumer right or for the business to verify the consumer’s identity. A business does not have a direct relationship with a consumer simply because the business collects brokered personal information directly from the consumer; the consumer must intend to interact with the business. A business is still a data broker and does not have a direct relationship with a consumer as to the brokered personal information the business sells about the consumer that it collected outside of a first-party interaction with the consumer.