

California Personal Information Disclosure

California Civil Code 1798.115(c), 1798.130(a)(5)(c), 1798.130(c), and 1798.140 indicates that companies should disclose whether the following categories of information are collected, transferred for consideration, or transferred for an organization's "business purpose" as that term is defined under California law. Note that while a category may be marked, that does not necessarily mean that we have information in that category about you. For example, while we transfer bank account numbers for our business purpose in paying our employees (e.g., direct deposit) we do not collect or transfer bank account numbers of individuals that submit questions on our website's "contact us" page. Please note that we do not "sell" personal information about California residents.

Categories of Personal Information That We Collect	Categories of Third Parties to Whom We Disclose Personal Information for Business Purpose
<p>Identifiers – such as name, postal address, phone number, unique personal identifier, online identifier, internet protocol (IP) address, device ID, email address, account name, signature, social security number, driver's license number, passport number, or other similar identifiers.</p>	<ul style="list-style-type: none"> • Service Providers • Product and service fulfillment companies • Internet service providers • Advertising Networks • Social Networks • Payment Processors and financial institutions Government entities, law enforcement, lawyers, auditors, consultants and other parties as required by law • Data analytics providers
<p>Financial information – such as bank account number, credit or debit card number, or other financial information.</p>	<ul style="list-style-type: none"> • Service Providers • Payment Processors and financial institutions Government entities, law enforcement, lawyers, auditors, consultants and other parties as required by law
<p>Medical and/or health insurance information – such as information from a healthcare provider regarding an individual's medical history, mental or physical condition, or treatment; an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in the individual's application and claims history.</p>	<ul style="list-style-type: none"> • Service Providers • Government entities, law enforcement, lawyers, auditors, consultants and other parties as required by law
<p>Protected characteristics – such as race, gender, physical or mental disability, and religion.</p>	<ul style="list-style-type: none"> • Service Providers • Government entities, law enforcement, lawyers, auditors, consultants and other parties as required by law
<p>Commercial information – such as information about products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.</p>	<ul style="list-style-type: none"> • Service Providers • Product and service fulfillment companies • Advertising Networks • Social Networks • Payment Processors and financial institutions Government entities, law enforcement, lawyers, auditors, consultants and other parties as required by law • Data analytics providers
<p>Network activity data – Internet or other electronic network activity information, such as browsing history,* search history, and information regarding an individual's interaction with an Internet website, application, or advertisement.</p>	<ul style="list-style-type: none"> • Service Providers • Product and service fulfillment companies • Internet service providers • Advertising Networks • Social Networks • Government entities, law enforcement, lawyers, auditors, consultants and other parties as required by law • Data analytics providers

<p>Biometric information – such as fingerprint, face print or voice print.</p>	<ul style="list-style-type: none"> • Service Providers • Government entities, law enforcement, lawyers, auditors, consultants and other parties as required by law
<p>Electronic and sensory data – such as audio, electronic, visual, thermal, olfactory, or similar information (e.g., pictures, a recording of a customer service call, security video surveillance footage).</p>	<ul style="list-style-type: none"> • Service Providers • Government entities, law enforcement, lawyers, auditors, consultants and other parties as required by law
<p>Professional/employment information – such as occupation and professional references.</p>	<ul style="list-style-type: none"> • Service Providers • Government entities, law enforcement, lawyers, auditors, consultants and other parties as required by law
<p>Inferences – drawn from any of the information listed above to create a profile</p>	<ul style="list-style-type: none"> • Service Providers • Advertising Networks • Social Networks • Government entities, law enforcement, lawyers, auditors, consultants and other parties as required by law • Data analytics providers
<p>California Customer Records – Medical and health-related data, such as body temperature, symptoms, vaccination status, and underlying health conditions (only applicable where a serious public health threat has been identified or as required by law).</p>	<ul style="list-style-type: none"> • Other Service Providers • Government entities, law enforcement, lawyers, auditors, consultants and other parties as required by law

* Please note that browsing history is used to ensure the functionality of our websites (e.g. to allow you to buy items and log in to your account) and for analytics (e.g. to improve the operation and layout of our website).