Overview of State Privacy Laws

On January 1, 2023, the California Privacy Rights Act (CPRA), an act amending the California Consumer Privacy Act (CCPA) of 2018, will go into effect, and a comprehensive privacy law will go into effect in Virginia. By the end of 2023, privacy laws in at least three other states (Colorado, Connecticut, and Utah) will go into effect. These laws amend and expand rights that consumers were afforded under the CCPA, add similar rights to new states, and create additional responsibilities relating to how LiveRamp handles personal data.

LiveRamp has always been a privacy-centric company focused on enabling the safe and effective use of data, and we welcome the passage of additional privacy laws. Many of the new state laws codify the policies and standards that LiveRamp has implemented for many years. As it was for the CCPA in 2018, LiveRamp is prepared to comply with the requirements of new state privacy laws when they go into effect, and we intend to serve as a trusted technology partner for our customers as we move forward in this process.

The table below provides information on what these requirements might mean for you and how LiveRamp is meeting these requirements.

Requirements	What This Means for Controllers (called "Businesses" in California)	How LiveRamp is Meeting this Requirement
Notice at Collection	Prior to or at the point of collection, consumers must be informed that data is being collected and the reason why the data is being collected.	LiveRamp data partners who have a direct consumer relationship are required to provide notice and choice in compliance with law. We also follow all notice and choice requirements applicable to LiveRamp through privacy notices and instructions for consumer rights and choices on our website.
Privacy Policy	A business's privacy policy must be updated at least once every 12 months and include information which describes consumers' rights under state privacy laws, methods for submitting consumer requests, and a list of the categories of personal data collected for the preceding 12 months.	LiveRamp's privacy policy has been updated to meet all of the requirements of the CCPA and will be updated as new state laws are made effective. It is easily accessible on our website here: https://liveramp.com/privacy/

Requirements	What This Means for Controllers (called "Businesses" in California)	How LiveRamp is Meeting this Requirement
Opt-Out & Website	For businesses that sell consumers' information, it is required that consumers are provided the right to opt-out of the sale of their personal data. Companies must provide a "Do Not Sell My Personal Information" link on the homepage that leads consumers to the opt-out process. Under the CCPA/CPRA, an individual has the right to opt out of "sharing", which means making personal data available for the purpose of cross-contextual behavioral advertising. Other state laws require an opt-out for "targeted advertising," which is similar in scope to the sharing opt-out.	LiveRamp's website includes all required language and a "Do Not Sell My Personal Information" link on the homepage. You can view this information by visiting https://liveramp.com/privacy/california-privacy-notice/your-rights/. LiveRamp's existing "Do Not Sell My Personal Information" options are available to California residents and will be expanded to other states as privacy laws are made effective. In addition, LiveRamp offers robust opt out options for residents of all states. An opt out at LiveRamp is comprehensive and is effective for all of the opt outs required under the new laws (i.e., selling, sharing, targeted advertising). If a consumer exercises their opt out rights with our customer, the customer must notify LiveRamp of the opt out, and we will process the request from the individual against the customer's workflows and keep a record of the opt out on the customer's file to apply to future processing.
Access	Upon a verifiable consumer request, a business must provide information regarding the categories of personal data collected, categories of sources from which the information is collected, the purpose for compiling the information, categories of third parties with which the business shares personal data, and specific pieces of personal data the business has collected.	LiveRamp is following best practices to ensure consumers are who they say they are when submitting a request. Upon confirmation of their identity, we share the required information including types, categories, and specific pieces of personal data. We also share information regarding the types of companies who utilize our data but not the names of actual clients.
Deletion	Upon the consumer's request, businesses must delete the data collected for that consumer.	LiveRamp has multiple workstreams in place to ensure data is deleted upon a consumer's request. If a consumer exercises their right to delete with our customer, the customer must notify LiveRamp of the deletion request, and we will process the request against the customer's data held by LiveRamp and make the deletion request available downstream to the customer and its partners.

Requirements	What This Means for Controllers (called "Businesses" in California)	How LiveRamp is Meeting this Requirement
Correction	Consumers have the right to request correction of inaccurate personal data that businesses hold about them. A business's response to a correction request must be commercially reasonable, taking into account the nature of the information and purposes of the processing.	For direct requests to LiveRamp from a consumer for correction, LiveRamp will delete the consumer's information. For "indirect" requests to correct consumer data controlled by a LiveRamp customer and for which LiveRamp is acting as a processor, LiveRamp will assist the customer by applying the requested correction to the data held by LiveRamp on behalf of our customer.
Limit the Use & Disclosure of Sensitive personal data	California gives consumers the right to direct a business to limit its use and disclosure of their sensitive data, with some exceptions. Businesses must provide a link on their websites entitled "Limit the Use of My Sensitive Personal Data," along with two or more methods to submit such requests. The requirement for a "right to limit" link is specific to California (CA), though sensitive data processing in general is subject to opt-in in Colorado (CO), Connecticut (CT), and Virginia (VA), and opt-out in Utah (UT).	In response to consumer requests to limit the use of their sensitive data, LiveRamp will record an opt out for the consumer and offer the option to further delete the personal data.
Opt Out of Profiling	In CO, CT, and VA, consumers have the right to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects. California provides a right to opt out of the use of automated decision-making technology, including profiling. It is expected that "automated decision-making" will be further defined through regulations. Utah does not provide a profiling opt-out.	Based on current laws and regulations, this requirement is not applicable to LiveRamp. LiveRamp will continue to monitor regulatory developments to determine applicability and to ensure we meet all necessary requirements.
Data Portability	Data provided to consumers under must be in a portable and, to the extent technically feasible, readily usable format.	Upon confirmation of consumer identity in response to a data access request, LiveRamp shares the required information and data as .csv files to ensure portability and usability.

Requirements	What This Means for Controllers (called "Businesses" in California)	How LiveRamp is Meeting this Requirement
Opt-Out Signals	CA, CO, and CT require businesses to allow consumers to opt out of the sale of their personal data through an opt-out "signal" that is transmitted by consumers' browsers and/or devices. California has proposed (but not yet finalized) requirements for such signals, and CO is considering its own standards. The opt-out signal provisions in CO and CT go into effect on July 1, 2024 and Jan. 1, 2025, respectively. Under the CCPA, businesses that require information such as a consumer's name and/or address to honor opt-out requests must continue to provide a "Do Not Sell My Personal Data" link.	All visitors of the LiveRamp website have the ability to opt-out of cookies to prevent retargeting through LiveRamp. In addition, LiveRamp pixel-based workflows are able to read and respond to various consent signals such as Global Privacy Control (GPC), the IAB US Privacy String, and the IAB TCF V2 Consent String. LiveRamp will also begin implementation of the multi-state IAB Global Privacy Platform consent string when it is finalized. We expect many companies to utilize these signals as the way for consumers to exercise the right to opt out of targeted advertising (e.g., "sharing" in California).
Anti- Discrimination	If a consumer chooses to enact any of their CCPA rights, a business may not discriminate against them for doing so.	LiveRamp complies with and responds to all verifiable consumer data privacy requests under CCPA.
Consent to Process Sensitive Data	In CO, CT, and VA, a business must obtain an individual's opt-in consent prior to processing his/her sensitive data. In CA and UT, sensitive data is subject to an opt-out, provided that the use of the data is compatible with the context and purposes defined at the point of collection.	While LiveRamp does not directly collect sensitive data, its data partners are required to provide notice and opt-out choices and obtain consent that meets applicable legal requirements.

Requirements	What This Means for Controllers (called "Businesses" in California)	How LiveRamp is Meeting this Requirement
Contracts with Third Parties	Under the revised CCPA, California will regulate contracts between businesses and businesses or third parties, i.e., situations that typically involve sales of personal data. Under the CCPA, contracts with third parties must: 1. Specify the purposes for which the third party may use the data. 2. Limit the third party's use of the data to such purposes. 3. Require the third party to comply with applicable obligations under the CCPA. 4. Permit the business the right to take reasonable and appropriate steps to ensure the third party's compliance with its obligations. 5. Permit the business to take reasonable and appropriate steps to stop the third party's use of personal data. 6.Require the third party to notify the business no later than 5 days after determining it can no longer meet its obligations.	LiveRamp is modifying contracts to comply with these requirements.
Contracts with Processors (called "Service Providers" in California)	State privacy laws impose a set of requirements on contracts between businesses and their processors (called "service providers" in California). In general, these requirements require the processor to act at the business's direction and prohibit the processor from using or retaining data received from the business for the processor's own benefit. There are also requirements for the processor to allow for reasonable due diligence and oversight by the controller ("business" in California).	When handling customer data as a processor, LiveRamp complies with these requirements and is updating applicable contracts to reflect the specific terms required by the new laws.
Data Protection Impact Assessments	Businesses that engage in sales of personal data, sensitive data processing, targeted advertising or profiling, or activities that present "significant" or "heightened" risk to consumers' privacy or security must perform data protection impact assessments.	LiveRamp conducts and documents privacy and security assessments for its products that meet these requirements.