

THE DEVIL IS IN THE DETAILS - PART II: CONSUMER RIGHTS UNDER U.S. DATA PRIVACY LAWS



Aviva Surugeon

Is the consumer always right? Maybe. But under the five states that have enacted comprehensive privacy laws, consumers have slightly varying ways in which to invoke these afforded rights. The California Privacy Rights Act (CPRA) (which amends and expands the California Consumer Privacy Act (CCPA)), Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA), Utah Consumer Privacy Act (UCPA), and Virginia Consumer Data Protection Act (VCDPA) will all take effect in 2023. Each will provide enumerated consumer data privacy rights. In Part I of this series, we outlined the general differences among the U.S. comprehensive data privacy laws that have been adopted. Here, we dig into how each State's law gives individuals more control over their personal information by providing certain consumer rights and what key distinctions covered businesses should be aware of concerning the varying States' laws.

COMMON CONSUMER RIGHTS

Notwithstanding a few deviations, the five comprehensive consumer privacy laws provide consumers with the following rights:

Right to confirm personal data are being processed.

Right to access their personal data.

Right to correct inaccuracies in their personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

Right to delete personal data provided by, or obtained about, the consumer. However, certain exceptions enumerated in each State's law may inhibit the consumer's right to deletion.

Right to data portability where consumers have the right to obtain a copy of the consumer's personal data processed by the controller in a readily usable format that allows the consumer to transmit the data to another controller without hindrance.

Right to opt out of the processing of the personal data for the purposes of:

- targeted advertising;
- the sale of personal data; or
- profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

THE DEVIL IS IN THE DETAILS - PART II: CONSUMER RIGHTS UNDER U.S. DATA PRIVACY LAWS



PAGE 2

KEY DISTINCTIONS

While providing similar consumer rights, the five different privacy laws feature notable differences. For example, the CPRA and UCPA afford deletion rights that are limited to personal information collected from the consumer. However, under the VCDPA, CPA, and CTDPA, any personal information collected about the consumer is in scope of the deletion right.

Also, the UCPA stands alone in not providing a right for consumers to appeal denials of requests to exercise their rights, correct personal data inaccuracies, or opt out of profiling. Notably, under the VCDPA and UCPA, the right to data portability is limited to consumer-provided data. However, CTDPA's approach is more like the CPA, allowing consumers to obtain a copy of the data a controller has processed about them regardless of how the controller acquired it.

The most notable differences surround the collection and processing of sensitive personal information. Under the CPRA, where a business collects or processes sensitive personal information for the purpose of inferring characteristics about a consumer, it will either need to self-restrict its use of that information to certain purposes set forth in the CPRA, or it will need to provide consumers with a notice and the right to limit the business's use of the information to the statutory purpose. However, under the VCDPA, CPA, and CTDPA, sensitive personal information is defined differently, requiring controllers to obtain consumer opt-in consent and conduct a data processing assessment before processing the information. The UCPA does not require consumer consent for processing sensitive data, and only requires that businesses provide notice and an opportunity to opt out of the use of sensitive data.

In addition to consumer rights, each State's law requires that organizations provide privacy notices regarding the categories and processing of consumers' personal data. But the CPRA is the only law requiring notice upon collection of data. Further, all five privacy laws require that the privacy notices include the categories of data, the purpose of processing the consumer's data, how the consumer can exercise their rights, and what data are shared with third parties and the types of third parties with whom the data are shared. However, the CPRA notice requirements include compliance with the rights to opt out of the sale of personal information or sale of personal information for targeted advertising, including placement of a "Do Not Sell or Share My Personal Information" link on the homepage of a company's website. Under the CTDPA, controllers are required to provide clear and conspicuous links on their websites that give consumers a choice to opt out of certain types of processing. Beginning January 1, 2025, however, controllers must recognize universal opt-out preference signals indicating a consumer's intent to opt out of targeted advertising and sales, which will trump any conflicting controller-specific privacy setting. The CPA similarly mandates recognition of universal opt-out signals, beginning July 1, 2024. But unlike CPA, the CTDPA does not require controllers to authenticate opt-out requests, which in theory, will make it easier for consumers to opt out.

THE DEVIL IS IN THE DETAILS - PART II: CONSUMER RIGHTS UNDER U.S. DATA PRIVACY LAWS



PAGE 3

Additionally, the CPRA includes the concept of “sharing,” which focuses on whether third parties use personal information for cross-context behavioral advertising, rather than on whether there is monetary or other valuable consideration for the disclosure – i.e., “selling.” Under the CPRA, “sharing” data involves the disclosure, transfer, or other communication of personal information to third parties for purposes of advertising that is targeted based on a consumer’s activities on third-party and distinctly branded digital platforms. Also of note, while the CPRA’s provisions do not take full effect until January 1, 2023, under the CPRA, the calendar year of 2022 is treated as a lookback period. This means that any personal data collected during 2022 is subject to the terms of the CPRA starting in 2023.

The chart below provides a handy comparison of the key consumer rights of each state’s law:

Consumer Right	CPRA	VCDPA	CPA	UCPA	CTDPA
Right to confirm personal data is being processed	Implied	✓	✓	✓	✓
Right to access	✓	✓	✓	✓	✓
Right to data portability	✓	✓	✓	✓	✓
Right to delete	✓	✓	✓	✓	✓
Right to correct	✓	✓	✓	X	✓
Right to opt out of sale	✓	✓	✓	✓	✓
Right to opt out of targeted/cross-context behavioral advertising	✓	✓	✓	✓	✓
Right to opt out of profiling	✓	✓	✓	X	✓
Right to limit use and disclosure of sensitive personal information	Opt Out	Opt In	Opt In	Notice + Option to Opt Out	Opt In
Notice at collection requirement	✓	X	X	X	X
Right to not be discriminated against for exercising rights	✓	✓	✓	✓	✓

THE DEVIL IS IN THE DETAILS - PART II: CONSUMER RIGHTS UNDER U.S. DATA PRIVACY LAWS



PAGE 4

Consumer Right	CPRA	VCDPA	CPA	UCPA	CTDPA
Privacy Notice Requirements	<p>Categories of data</p> <p>Purpose of processing</p> <p>How to exercise rights</p> <p>Categories of data shared with third parties</p> <p>Categories of third parties with whom data is shared</p> <p>Any sale of data and how to opt out</p> <p>Clear and conspicuous link to opt out of sale on homepage</p> <p>Duration of retention period for data</p> <p>Notice to consumers of their CPRA rights</p> <p>Categories of sources of data</p> <p>Categories of sensitive personal data, and consumer's right to opt out of use</p>	<p>Categories of data</p> <p>Purpose of processing</p> <p>How to exercise rights</p> <p>Categories of data shared with third parties</p> <p>Categories of third parties with whom data is shared</p> <p>Any sale of data or targeted advertising and how to opt out</p>	<p>Categories of data</p> <p>Purpose of processing</p> <p>How to exercise rights</p> <p>Categories of data shared with third parties</p> <p>Categories of third parties with whom data is shared</p> <p>Any sale of data and how to opt out</p>	<p>Categories of data</p> <p>Purpose of processing</p> <p>How to exercise rights</p> <p>Categories of data shared with third parties</p> <p>Categories of third parties with whom data is shared</p> <p>Any sale of data or targeted advertising and how to opt out</p>	<p>Categories of data</p> <p>Purpose of processing</p> <p>How to exercise rights</p> <p>Categories of data shared with third parties</p> <p>Categories of third parties with whom data is shared</p> <p>Any sale of data or targeted advertising</p> <p>Clear and conspicuous link to a webpage for opting out of sale or targeted advertising</p> <p>Active email address for how to contact the controller</p>
Timing to Respond	<p>45 days, with an additional 45 days when reasonably necessary</p> <p>15 days for opt-out requests</p>	<p>45 days, with an additional 45 days when reasonably necessary</p>	<p>45 days, with an additional 45 days when reasonably necessary</p>	<p>45 days, with an additional 45 days when reasonably necessary</p>	<p>45 days, with an additional 45 days when reasonably necessary</p>
Right to Appeal	✓*	✓	✓	X	✓

*There is no statutory right to appeal, however, CPRA §1798.145(h)(2) suggests appeal processes are at the option of the business.

THE DEVIL IS IN THE DETAILS - PART II: CONSUMER RIGHTS UNDER U.S. DATA PRIVACY LAWS



PAGE 5

LOOKING AHEAD

As 2023 quickly approaches, organizations need to be mindful of these nuanced differences in consumer rights afforded under each of the five privacy laws. Ultimately, organizations should be wary of a one-size-fits-all method in perfecting compliance. Redgrave LLP will continue to monitor the changing landscape of U.S. data privacy legislation and is available to consult and assist in developing and deploying successful information governance and privacy policies and practices.

For assistance with or additional information on this topic, please contact Martin Tully at mtully@redgravellp.com or Eliza Davis at edavis@redgravellp.com.

Redgrave LLP is one of the largest legal practices focused exclusively on addressing the legal challenges that arise at the intersection of the law and technology, including eDiscovery, information governance, and data privacy. We employ some of the most experienced professionals in the field. We provide clients with practical, innovative, and cost-effective solutions and serve Global and Fortune 500 companies across a diverse array of industries. We also work collaboratively with Am Law 100 law firms in roles ranging from co-counsel to consulting and testifying expert witnesses and have appeared in state and federal courts throughout the United States.