DAVIS GILBERT

Privacy + Data Security

Utah Consumer Privacy Act Joins the Growing List of Comprehensive State Privacy Laws

The Bottom Line

- In the absence of a new comprehensive consumer privacy law on the federal level, states continue to propose their own laws.
- Utah has become the fourth state in the United States to enact such a law.
- There are similarities, but some differences, with the new laws in California, Virginia and Colorado. Therefore, compliance continues to get more complex for businesses.

Following in the footsteps of California, Virginia and Colorado, Utah has become the fourth state in the United States to enact a comprehensive consumer privacy law. Governor Spencer Cox signed the Utah Consumer Privacy Act (UCPA) into law on March 24, 2022. The new law will go into effect on December 31, 2023, shortly after the effective dates of new privacy laws in California, Virginia and Colorado.

Threshold Requirements

The UCPA applies to "any controller or processor" that conducts business in the state or produces products or services targeted to state residents, and that controls or process the personal data of at least:

- 100,000 consumers during a calendar year; or
- 25,000 consumers and derives over 50 percent of gross revenue from the "sale" (defined below) of personal data.

The controller or processor also must have an annual revenue of $25,000 or more. A similar monetary threshold can be found in the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), but is absent from the Virginia Consumer Data Protection Act (CDPA) and the Colorado Privacy Act (CPA).

Consumer Rights

Similar to the CPRA, CDPA and CPA, the UCPA provides consumers a series of rights regarding their personal data:

rights of access, deletion, data portability and the right to opt out of targeted advertising or sales of personal data. However, the UCPA does not include a right to correction, which the other three state laws do include, and the UCPA's right to deletion is limited to personal data that the consumer has provided directly to the controller. The UCPA does not give consumers the right to opt out of profiling, which the CDPA and CPA do allow, and, unlike the CPA, the UCPA does not recognize universal opt-out signals (such as the global privacy control) as a method for consumers to exercise their opt-out rights.

Sales of Personal Data

The UCPA grants Utah residents the right to opt out of the sale of their personal data. However, the Utah law narrowly defines the "sale" of personal data as "the exchange of personal data for monetary consideration by a controller to a third party," and excludes non-monetary forms of consideration from the definition. Similar to the CDPA and CPA, the UCPA also makes several exemptions from the definition of "sale," including disclosures to affiliates and disclosures at the direction of the consumer. However, the UCPA goes further than the CDPA and CPA by exempting disclosures to third parties that are "consistent with a consumer's reasonable expectations" depending on "the context in which the consumer provided the personal data to the controller."

Duties for Controllers

Controllers under the UCPA share many of the same duties prescribed under the CPRA, CDPA, and CPA, including the duty to:

- Provide a privacy policy that includes: the categories of personal data processed and shared with third parties; the purposes for processing personal data; a description of how consumers may exercise their rights; and the categories of third parties, if any, with whom the controller shares personal data;
- "Clearly and conspicuously disclose" to consumers the ways in which they may opt out of sales of their personal data or processing for targeted advertising;
- Establish, implement and maintain reasonable administrative, technical and physical data security practices; and
- Not discriminate against consumers for exercising their rights.

Unlike the CPRA, CDPA and CPA, the UCPA does not require that controllers conduct "risk assessments" or "data protection assessments." Moreover, while controllers must enter into data protection agreements with processors, the law mandates fewer requirements than

the other state privacy laws. Notably absent are requirements that processors comply with reasonable audits or assessments by, or delete or return all personal data to, the controller.

Sensitive Data

The UCPA criteria for "sensitive data" mirrors the CDPA in large part, including personal data that reveals an individual's racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, medical history, mental or physical health conditions, medical treatment/diagnosis and specific geolocation data. Under the UCPA, controllers cannot process sensitive data collected from a consumer without providing a "clear notice and an opportunity to opt out of the processing" (with the exception of children's data, which requires affirmative consent). While this requirement is less restrictive than the CDPA's and CPA's opt-in requirements, the ability for consumers to opt out altogether appears more consumer-friendly than the CPRA's right to limit the use and disclosure of such information.

Enforcement

There is no private right of action under the UCPA, and a violation of the UCPA cannot be used to support a private right of action under any other Utah laws.

The Utah Attorney General (Attorney General) has exclusive authority to enforce the UCPA, although such enforcement powers are more circumscribed than under the California, Virginia and Colorado laws. The UCPA provides that enforcement actions by the Attorney General may be initiated "[u]pon referral from" the Utah Division of Consumer Protection (Division). The net effect of this is that the Attorney General does not have independent authority or discretion to investigate and pursue violations of the UCPA on its own. Instead, the Division must receive a consumer complaint, conduct an investigation, and only refer the matter to the Attorney General on "reasonable cause" that "substantial evidence" supports a finding of the violation identified in the consumer complaint. Even then, the Attorney General has to issue a formal notice of violation and grant the target business 30 days to cure before bringing an enforcement action. The sum total of these requirements creates a more business-friendly process.

Violations that have not been cured within 30 days are subject to a fine of up to $7,500 per violation. If there are multiple parties involved in the same data processing violation, liability under the UCPA is allocated among the parties according to the principles of comparative fault.

Privacy + Data Security

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Zachary N. Klein

Associate
212 237 1495
zklein@dglaw.com