Data Privacy and Cybersecurity

Utah Set to Enact Comprehensive Consumer Privacy Law

By: Madeleine V. Findley and Xinyue (Dagny) Lu

Utah is poised to become the fourth state to pass comprehensive consumer privacy legislation, after California, Virginia, and Colorado. The Utah Consumer Privacy Act (UCPA) was approved by the Utah House of Representatives on March 2 after clearing Senate approval last week. If enacted, the UCPA would take effect on December 31, 2023.

The UCPA would impose data protection obligations on those who process the personal data of Utah residents. It would also afford Utah residents corresponding rights and remedies. Enforcement would be handled by the Utah Attorney General and provides a 30-day cure period. The law does not contain a private right of action or require data processing impact assessments.

Who Must Comply with the UCPA?

The UCPA would apply to entities conducting business in Utah or targeting Utah consumers with their products or services, and that (1) have an annual revenue of $25,000,000 or more and (2) either (a) control or process the personal data of at least 100,000 consumers in a year; or (b) derive over 50% of its gross revenue from the sale of personal data and control or process the personal data of at least 25,000 consumers. These thresholds closely mirror the Virginia Consumer Data Protection Act passed in 2021.

The UCPA contains several notable exemptions. It would not apply to (1) government entities and their contractors, (2) tribes, (3) higher education institutions, (4) nonprofit organizations, (5) entities already regulated under the Health Insurance Portability and Accountability Act (HIPAA) and related regulations, (6) financial institutions already regulated by the Gramm-Leach-Bliley Act, (7) air carriers, or (8) private individuals processing data for purely personal or household purposes. The UCPA also would not apply to certain consumer credit reporting activities that are regulated by the federal Fair Credit Reporting Act.

What Data Does the UCPA Protect?

The UCPA would protect "personal data," which is defined as "information that is linked or reasonably linkable to an identified individual or an identifiable individual." Personal data does not include deidentified data, aggregated data, or publicly available information.

The UCPA would also exempt several categories of data subject to other sector-specific privacy laws, including (1) certain health, health care, patient, and research subject information protected by other federal laws (including HIPAA); (2) personal data governed by the federal Driver's Privacy Protection Act of 1994; (3) personal data regulated by the federal Family Education Rights and Privacy Act and related regulations; (4) personal data governed by the federal Farm Credit Act of 1971; and (5) certain employee information.

What Are a Business's Obligations Under the UCPA?

To comply with the UCPA, a business would be generally required to implement data security practices to safeguard personal data, and enter data processing contracts with vendors and service providers that contain certain required provisions. A business may also be required to update its privacy policy (or create a privacy policy) to reflect its Utah personal data processing activities, disclose the rights

available to Utah residents under the UCPA, and communicate how Utah residents may exercise those rights.

Businesses processing a resident's "sensitive data" are required to first provide the resident with clear notice and an opportunity to opt-out of the processing. The UCPA defines "sensitive data" to include personal data that reveals a person's racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, medical history, genetic or biometric information, or specific geolocation.

What Rights Do Utah Residents Have Under the UCPA?

The UCPA would afford Utah residents several rights with respect to a business's processing of their personal data, including the right to (1) confirm whether the business is processing their personal data; (2) access their personal data; (3) request that the business delete their personal data; (4) obtain copies of the personal data they have provided to the business; and (5) direct the business to not process their personal data for targeted advertising or sale.

A resident may exercise any such rights by submitting a request to the business. The business has an initial period of 45 days to respond to an authenticated request, which may be extended for an additional 45 days. Residents may generally make one request to each business each year for free, and businesses may impose charges for additional requests or excessive or bad faith requests.

How do the Rights Under the UCPA Compare to Those in Other States?

The UCPA tracks more closely to the privacy laws enacted in Virginia and Colorado than to California's model. It would provide for privacy rights that are similar to, but narrower than, the ones found in the Virginia Consumer Data Protection Act (VCDPA) and Colorado Privacy Act (CPA). Unlike the VCDPA or CPA, the UCPA does not provide consumers with a right to request correction of their personal data, or the right to opt out of profiling. Businesses that process sensitive data would be required to provide notice and an opportunity to opt-out but would not have to obtain consent to such processing. Additionally, an individual's right to delete personal data under the UCPA is limited to data the individual has provided to the business, and does not extend to data the business has obtained from other sources. Lastly, the UCPA adopts a narrower definition of "sale" of personal data than other state privacy laws that would exclude a business's disclosure of a Utah resident's personal data to third parties if "the purpose [of the disclosure] is consistent with [the resident's] reasonable expectations" when taking into account "the context in which the [resident] provided the personal data to the [business]."

The UCPA does not include California-style rights to opt-out of the sale or "sharing" of personal data, automated decision-making technology, or to limit the use and disclosure of a significantly broader range of "sensitive personal information." It also does not require businesses to recognize the Global Privacy Control.

How is the UCPA Enforced?

The Utah Attorney General would have the exclusive authority to enforce the UCPA. Consumers may bring complaints about alleged violations to the Utah Department of Commerce's Division of Consumer Protection, which can investigate and refer complaints to the Utah Attorney General. The UCPA expressly states that it does not create a private right of action.

The Attorney General would be required to provide businesses with a 30-day cure period for any alleged violation. The Attorney General is not required to provide additional opportunities to cure for subsequent violations by the same business. The right-to-cure provision does not sunset.

The Attorney General would have authority to seek civil penalties, including actual damages plus a fine not exceeding $7,500 per violation of the UCPA.

Next Steps

The Utah House and Senate bills, which are largely identical, must be reconciled by March 4, the last day of the legislative session. The Governor will then have until March 24 to sign or veto the bill.

Contact Us

Madeleine V. Findley

mfindley@jenner.com | Download V-Card

Xinyue (Dagny) Lu

xlu@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower

Co-Chair

dbitkower@jenner.com

Download V-Card

Madeleine V. Findley

Co-Chair

mfindley@jenner.com

Download V-Card