Updates
March 31, 2022

Utah Joins California, Colorado, and Virginia With Omnibus Privacy Law

Utah Governor Spencer Cox signed the Utah Consumer Privacy Act (Utah Law) into law on March 24, 2022, making it the fourth omnibus state privacy law enacted in the United States. California led with the California Consumer Privacy Act (CCPA), which was amended by the California Privacy Rights Act of 2020 (CPRA), followed by the Virginia Consumer Data Protection Act (Virginia Law), and the Colorado Privacy Act (Colorado Law). The CPRA, Virginia Law, and Colorado Law each go into effect in 2023, with the Utah Law becoming effective at the end of the year on December 31, 2023.

The Utah Law largely follows the structure and terminology found in Virginia and Colorado's privacy laws. It similarly provides consumers with rights to their data, requires opt outs for certain processing, and distinguishes between data controllers and processors. However, the Utah Law is more business-friendly than existing omnibus state privacy laws, in that it generally provides fewer consumer rights and company obligations. It also does not cover consumers acting in an employment or commercial context, contains no private right of action, and provides companies with a mandatory 30-day cure period.

This update provides an overview and summary of the main aspects of the Utah Law, with comparisons to existing omnibus state privacy laws. It also provides recommendations on how companies that may be subject to the Utah Law can prepare for compliance.

Scope and Applicability

The Utah Law Applies to Utah Businesses and Businesses Outside of Utah

The Utah Law applies to a "controller" or "processor" that conducts business in Utah, *or* that targets products or services to consumers in Utah and

- Has an annual revenue of $25 million or more; and
- Satisfies one or both of the following thresholds:
    - Controls or processes the personal data of 100,000 or more Utah consumers during a calendar year; *or*
    - Derives over 50% of its gross revenue from selling personal data and controls or processes the personal data of 25,000 or more Utah consumers.

Notably, the Utah Law differs from existing omnibus state privacy laws by requiring businesses to have $25 million or more in annual revenue to fall under the law, *in addition to* satisfying at least one other threshold. It contains similar definitions for a "controller" and "processor" as those found in the Colorado and Virginia laws. Under the Utah Law, a "controller" is an entity that does business in Utah that alone or jointly with others, determines the purposes for and means by which personal data is processed, and a "processor" is an entity that processes personal data on behalf of a controller.

The Utah Law Contains Numerous Listed Exceptions

The Utah Law contains exceptions that exclude certain types of entities, information, and activities. For instance, the Utah Law does not apply to government entities, tribes, higher education institutions, or nonprofit corporations. Similarly, it does not apply to protected health information (PHI) governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other personal data that is subject to certain federal laws (among them the Gramm-Leach-Bliley Act (GLBA), the Federal Credit Reporting Act (FCRA), and the Family Educational Rights and Privacy Act of 1974 (FERPA)).

Like the Colorado and Virginia laws, the Utah Law also excludes de-identified and publicly available information from the definition of personal data, but also goes one step further to exclude aggregated data. "Aggregated data" is broadly defined as information that relates to a group or category of consumers from which individual consumer identities have been removed and that is not linked or reasonably linkable to any consumer.

Data Rights

Following the framework for existing omnibus state privacy laws, the Utah Law gives consumers similar rights to know, access, and delete personal data held by a controller, as well as the right to data portability and to opt out of targeted advertising and the sale of personal data. The Utah Law's definition of "sale" of personal data is narrow and requires money to be exchanged. It further narrows activities that may be considered sales by excluding disclosures of personal data if the purpose of the disclosure is consistent with a consumer's "reasonable expectations," which is a much broader carveout than any found in existing omnibus state privacy laws. Notably, there is no right to correct inaccurate data or right to opt out of certain profiling activities, which is another departure from certain U.S. privacy legislation.

Like the Colorado and Virginia laws, the Utah Law does not extend consumer privacy rights to pseudonymous data, defined as "personal data that cannot be attributed to a specific individual without the use of additional information." Practically speaking, this means that when controllers respond to rights, such as access or deletion requests, they can exclude pseudonymous information that is kept separately and is subject to appropriate technical and organizational measures to prevent attribution.

Privacy Obligations

Controllers must post a privacy notice that contains disclosures about their personal data practices similar to those required under existing omnibus state privacy laws. For example, controllers must disclose the categories of personal data processed, purposes of processing, how consumers may exercise their rights, the categories of personal data disclosed to third parties, and the categories of third parties with whom personal data is shared. Additionally, controllers and processors must enter into a written contract that contains similar provisions to those required under other omnibus state privacy laws. Processors must also engage subprocessors pursuant to a written agreement that contains the same obligations as the processor with respect to the personal data.

Obligations Related to Sensitive Data

While the Colorado and Virginia laws require opt-in consent to process sensitive data, under the Utah Law, controllers need only provide notice and an opportunity to opt out prior to processing sensitive data (or, for the sensitive data of children under 13, comply with the Children's Online Privacy Protection Act (COPPA)), as is the case under the CPRA. Sensitive data includes data that reveals racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, medical history or health condition, genetic or biometric data used to identify specific individuals, and geolocation data. Note, however, that "sensitive data" under the Utah Law does not apply to information that reveals racial or ethnic origin when processed by a video communication

service, or by certain healthcare workers, which is a broader carveout than those found in the Colorado and Virginia laws.

How to Prepare

Companies that have already taken steps to comply with existing omnibus state privacy laws will have a head start when it comes to developing a compliance program that speaks to the Utah Law. The rights and obligations introduced by the Utah Law largely track the requirements under these other state laws.

For example, as with the Virginia and Colorado laws, companies should assess their use of personal data to determine what opt-out rights may need to be provided, particularly for sales and targeted advertising. Companies should also plan to update and roll out consumer-facing privacy notices. There may also be a need to provide just-in-time privacy notices, and opt-out notices for sales, targeted advertising, and processing of sensitive data.

Additionally, companies should review and update user interfaces and related processes for consumer rights requests to ensure compliance with the response parameters of these rights.

Companies should also take inventory of vendor contracts and prepare to update those with service providers, contractors, and other third parties that buy or receive personal data to ensure appropriate restrictions and obligations are in place. For help preparing for the Utah Law, please consult with experienced privacy counsel.

Authors

Miriam Farhi

Partner
MFarhi@perkinscoie.com 206.359.8195

Charlotte D. Kress

Associate
CKress@perkinscoie.com 202.654.1760

Explore more in

Privacy & Security Technology Transactions & Privacy Law Communications

Related insights

Update

A Greener Holiday Future: California Establishes Nation’s First Apparel and Textile Article EPR Program

Update

FERC Meeting Agenda Summaries for October 2024