ECKERT SEAMANS ATTORNEYS AT LAW

April 4, 2022

Data Security & Privacy Alert

Utah's New Consumer Privacy Law: What Businesses Should Know

By Sandy B. Garfnkel and Emma M. Lonbard

On March 24, 2022, Utah became the fourth and most recent state to enact a comprehensive consumer privacy law, the Utah Consumer Privacy Act ("UCPA"). After unanimous passage by both the Utah Senate and House, Governor Spencer Cox signed the bill (SB 227) into law, which will become effective on December 31, 2023. The UCPA largely mirrors the 2021 Virginia Consumer Data Protection Act and incorporates the familiar distinctions of "controllers" and "processors" originally found in Europe's General Data Protection Regulation ("GDPR"). Utah is the fourth U.S. state to adopt a consumer privacy law, preceded by California, Virginia and Colorado.

The UCPA defines "personal data" as "information that is linked or reasonably linkable to an identified individual or identifiable individual." It excludes "deidentified data, aggregated data, or publicly available information," while including pseudonymous data. It creates a category of "sensitive data" that includes personal data that reveals an individual's: racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, as well as information regarding an individual's medical history, diagnosis, treatment, or mental or physical health condition.

The UCPA applies to any controller or processor of personal data who (a) conducts business in Utah; or (b) who produces a product or service that is targeted to Utah residents, and has an annual revenue of $25,000,000.00 or more; and also satisfies one of the following thresholds: (i) during a calendar year, controls or processes personal data of 100,000 or more consumers; or (ii) derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers. There are exemptions for businesses engaged in activities that are regulated under certain federal privacy laws.

The UCPA grants consumers rights of data access, portability, and deletion concerning their personal data, as well as the right to opt-out of the sale of personal data, but does not include a right to correction. It provides a right to opt-out of the processing of their personal data for purposes of targeted advertising or sale. "Sale" is defined narrowly as "the exchange of personal data for monetary consideration by a controller to a third party." The following actions fall outside the scope of "sale": (1) a controller's disclosure of personal data to an affiliate; (2) disclosures to a processor who processes the data on behalf of the controller's behalf; (3) disclosures that are consistent with the consumer's reasonable expectations; (4) disclosures directed by the consumer; (5) disclosures to provide a product or service; and (6) disclosure as part of a transfer of assets during a proposed or actual merger, acquisition, or bankruptcy in which the third party assumes control of all or part of the controller's assets.

The Act does not provide consumers with a private right of action, but instead vests enforcement authority with the Utah Office of Attorney General. The statute provides a 30-day cure period after receiving written notice from the Attorney General of a violation. Penalties per violation include the actual damages to the consumer and up to $7,500 statutory penalty per violation.

Duties of Controllers

To comply with the Act, a controller who "sells" personal data to a third party or engages in targeted advertising must "clearly and conspicuously disclose" how consumers may exercise their opt-out rights. Except as otherwise provided, a controller may not process "sensitive data" collected from a consumer without "first presenting the consumer with clear notice and an opportunity to opt out of the processing; or for personal data of a known child, processing the data in accordance with [COPPA]." Controllers must "establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to (i) protect the confidentiality and integrity of personal data; and (ii) reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data." A data security program should reflect the "controller's business size, scope, and type," and should use data security practices appropriate "for the volume and nature of the personal data at issue." Also, a controller may not discriminate against consumers for exercising their consumer rights.

Duties of Processors

A processor must "adhere to the controller's instructions" for processing. Processors must assist controllers in meeting their obligations, including those related to the security of processing personal data and breach notification requirements, insofar as reasonably practicable. Prior to processing personal data on the controller's behalf, the processor must execute a data processing agreement with the controller that:

- clearly sets forth instructions for processing personal data, the nature and purpose of the processing, the type of data subject to processing, the duration of the processing, and the parties' rights and obligations;
- requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data; and
- requires the processor to engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations as the processor with respect to the personal data.

ECKERT SEAMANS ATTORNEYS AT LAW

This Data Security & Privacy Alert is intended to keep readers current on developments in the law. It is not intended to be legal advice. If you have any questions, please contact Sandy Garfinkel at 412.566.6868 or sgarfinkel@eckertseamans.com or Emma M. Lombard at 609.989.5024 or elombard@eckertseamans.com, or any other attorney at Eckert Seamans with whom you have been working.