BLANKROME

Privacy, Security & Data Protection

MARCH 28, 2022 • NO. 2

Utah Becomes the Fourth State to Pass Comprehensive Privacy Law

Following in the footsteps of California, Virginia, and Colorado, Utah has become the fourth state to pass its own comprehensive privacy law. On March 24, Utah officially enacted the Utah Consumer Privacy Act ("UCPA") after Utah Governor Spencer Cox signed the UCPA into law. Of all its predecessors, the UCPA's requirements most closely track the requirements of the Virginia Consumer Data Privacy Act ("VCDPA"). The UCPA will take effect December 31, 2023.

APPLICABILITY

The UCPA protects consumers' "personal data," defined as "information that is linked or reasonably linkable to an identified individual or an identifiable individual." The UCPA defines "consumer" as a Utah resident acting in an individual or household context and explicitly excludes individuals acting in an employment or commercial context, mirroring the approach of the VCDPA and the Colorado Privacy Act ("CPA").

The UCPA applies to entities that (a) conduct business in Utah or produce a product or service targeted to Utah residents; (b) have annual revenue of $25 million or more; and (c) satisfy one or more of the following thresholds: (i) control or process the personal data of 100,000 or more consumers or (ii) derive over 50 percent of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.

EXEMPTIONS

The UCPA provides for exemptions for several entities, such as government entities, nonprofit corporations, tribes, institutions of higher education, covered entities and business associates governed under the Health Insurance Portability and Accountability Act ("HIPAA"), and air carriers. Additionally, it exempts information governed by federal laws such as HIPAA, the Fair Credit Reporting Act ("FCRA"), the Gramm-Leach-Bliley Act ("GLBA"), the Driver's Privacy Protection Act, and the Family Education Rights and Privacy Act ("FERPA").

CONTROLLERS AND PROCESSORS

Like the VCDPA and CPA, the UCPA distinguishes controllers (*i.e.,* the entity that determines the purposes for and the means by which personal data is processed) and processors (*i.e.,* the entity that processes personal data on behalf of a controller). Controllers bear most responsibilities under the UCPA, such as having to respond to consumer requests to exercise their rights provided under the UCPA, as well as having to provide consumers with a reasonably accessible and clear privacy notice that discloses the controller's privacy practices. Unlike the VCDPA and CPA, the UCPA does not require controllers to perform data processing assessments.

Processors have direct obligations to adhere to the controller's instructions on processing personal data and to assist the controller in meeting the controller's obligations, including obligations related to the security of processing personal data and notification of a breach of security system under Utah's breach notification law.

Like the VCDPA and CPA, before a processor performs processing on behalf of a controller, the controller and processor must enter into a contract that clearly: (a) 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; (b) requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data; and (c) 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. However, unlike the VCDPA and CPA, the UCPA does not require contracts with processors to include provisions mandating that processors allow for or contribute to reasonable audits or require processors to make available to the controller information necessary to demonstrate compliance with the UCPA. Contracts with processors also do not need to require processors to delete or return all personal data to the controller at the end of the provision of services.

CONSUMER RIGHTS

The UCPA provides standard consumer rights—the rights to access and delete personal data, data portability, and the right to opt out of the processing of personal data for the purposes of targeted advertising and opt out of the sale of personal data. "Sale" under the UCPA is defined as the exchange of personal data for *monetary consideration* by a controller to a third party. This is much more limited than the expansive definitions of "sale" under the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA") and the CPA. Additionally, the UCPA does not require controllers to recognize global opt-out signals.

Similar to the VCDPA and CPA, the UCPA requires controllers to respond to a consumer request within 45 days of receipt of the request, which may be extended by an additional 45 days (for a total of 90 days) provided the extension is reasonably necessary and the controller informs the consumer of the extension, including the length of extension and the reasons for the extension. Controllers do not have to comply with a consumer request if the controller cannot authenticate the consumer request using commercially reasonable efforts.

SENSITIVE DATA; CONSENT

Unlike the VCDPA and CPA, which require opt-in consent for the processing of sensitive personal data, the UCPA only requires controllers to provide consumers notice and an opportunity to opt out of the processing of sensitive data. Under the UCPA, "sensitive data" is defined as personal data that reveals an individual's racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status; or information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a healthcare professional; geolocation data; and genetic personal data or biometric data if used for the purpose of identifying a specific individual. The UCPA only requires opt-in consent in the context of parental consent for the processing of personal data of children under 13.

Unlike the CCPA and CPA, the UCPA's definition of consent does not specifically exclude agreements obtained through dark patterns, which are user interfaces designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

ENFORCEMENT

Unlike the CCPA, the UCPA does not provide for a private right of action and explicitly precludes consumers from using a violation of the UCPA to support a claim under other Utah laws, such as laws regarding unfair or deceptive acts or practices, which has been a favorite tactic of plaintiffs' counsel. However, the UCPA establishes the Division of Consumer Protection ("Division") to which consumers may submit complaints regarding a controller's or processor's alleged violation of the UCPA and the Division has the authority to investigate the consumer complaint. If the director of the Division has reasonable cause to believe that substantial evidence exists that a controller or processor is in violation of the UCPA, the director may refer the matter to Utah's attorney general, who has the exclusive authority to enforce the UCPA. This two-step enforcement process is unique among comprehensive state privacy laws that have been passed to date. However, the Division must also provide consultation and assistance to the attorney g0eneral in enforcing the UCPA. The UCPA provides for a 30-day cure period.

KEY TAKEAWAYS

At least 24 states have introduced or re-introduced comprehensive privacy legislation during their 2022 sessions. Businesses should expect to see continued efforts to pass such laws and continue to closely monitor the developments on the state level. Unless and until the federal government passes preemptive legislation, the complex patchwork of state data privacy and security laws will continue to expand and create compliance challenges for national businesses.

To develop a data privacy and security compliance program that is flexible and able to evolve with the ever-changing legal landscape, businesses should invest in conducting robust data inventories to document the types of personal data collected and processed by the business, where the data is stored, the business purposes for collection, and with whom the data is shared. This will allow for the design and implementation of efficient, scalable processes to respond to consumer rights requests, help inform the prioritized deployment of safeguards to protect the data, and facilitate accurate and comprehensive notices to consumers that comply with the myriad applicable requirements. Businesses should also be sure to limit the scope of the personal data it collects, uses, or discloses to the minimum necessary to accomplish the intended purpose of the collection, use, or disclosure. Additionally, businesses should document their compliance efforts and maintain security procedures and practices to protect the data it collects and processes.

For more information or assistance, contact:

Sharon R. Klein
949.812.6010 | sharon.klein@blankrome.com

Alex C. Nisenbaum
949.812.6011| alex.nisenbaum@blankrome.com

Karen H. Shin
949.812.6012 | karen.shin@blankrome.com