Articles + Publications | May 16, 2022

Privacy Is the Buzz in the Beehive State: Utah's Consumer Privacy Act

Privacy & Cybersecurity Newsletter

WRITTEN BY

Niya T. McCray | Theodore P. Augustinos

As was widely predicted in the wake of the California Consumer Privacy Act, comprehensive privacy legislation continues to ripple out across the various states in 2022. Utah has become the fourth state, joining California, Colorado and Virginia, to enact sweeping consumer privacy legislation.

On March 24, 2022, the Utah Consumer Privacy Act (the "UCPA") was signed into law by Governor Spencer Cox. Businesses subject to the UCPA will have until December 31, 2023 to achieve compliance. Fortunately for businesses subject to the consumer privacy laws in California, Colorado and/or Virginia, the UCPA has many similarities.

Who is Subject to the UCPA?

Similar to the consumer privacy laws in Colorado and Virginia, the UCPA will apply to both data controllers and processors. Under the UCPA, a controller is "a person doing business in the state who determines the purposes for which and means by which the personal data is processed, regardless of whether the person makes the determination alone or with others."[1] Also similar to the Colorado and Virginia statutes, a processor is "a person who processes personal data on behalf of a controller."[2]

The UCPA will apply to data controllers that generate over $25 million in annual revenue and that either (i) control or process personal data for over 100,000 consumers yearly, or (ii) control and process personal data for over 25,000 consumers and generate over half of their revenue from selling personal data[3]. Here, the UCPA again mimics the Colorado and Virginia statutes in broadly defining personal data to include information that is linked or reasonably linkable to an identified individual or an identifiable individual.

Also similar to the Colorado and Virginia statutes, the UCPA sets forth important exemptions. First, the UCPA provides important exemptions for personal data collected from and about personnel and business to business ("B2B") contacts, as persons acting in a "commercial or employment context" are explicitly excluded from the UCPA's definition of consumers.[4]

The UCPA also provides several entity-based exclusions, including for entities regulated by the Gramm-Leach-Bliley Act ("GLBA"), and for covered entities and business associates as defined the Health Insurance Portability and Accountability Act ("HIPAA").[5]

©2026 Troutman Pepper Locke

The UCPA also provides information-level exclusions, including (i) protected health information as defined under HIPAA, (ii) activity by a consumer reporting agency that is subject to regulation by the Fair Credit Reporting Act ("FCRA"), and (iii) personal data regulated the Family Education Rights and Privacy Act ("FERPA").[6]

Consumer Rights

The UCPA provides a slate of consumer rights similar to those in Colorado and Virginia, and in California once the pending amendments take effect at January 1, 2023.[7] Consumers will have the rights to (i) know when a controller is processing and/or accessing their data, (ii) delete personal data, (iii) obtain and review their data, and (iv) opt out of the processing of their personal data to the extent it relates to targeted advertising and the sale of personal data. Unlike the other states, however, Utah does not provide consumers a right to correct inaccuracies in their personal data. Unlike the California, Colorado and Virginia statutes, which specify the means for submitting consumer requests, under the UCPA, the controller will be able to establish the requirements for submitting consumer rights requests.[8]

Controllers must respond to consumer requests within 45 days, or extend the initial response period by an additional 45 days.[9] Consumer requests believed to be fraudulent, excessive, unfounded, or unduly burdensome can be rejected, but the controller will bear the burden of demonstrating that it is not required to comply with the request.[10]

Controller Requirements

The UCPA imposes several requirements on controllers. Controllers are required to provide consumers with reasonably accessible and clear privacy notices that disclose the categories of personal data being processed, the purposes of data processing, consumer rights pursuant to the UCPA, and information on sharing with third-parties.[11]

The UCPA also requires controllers to protect personal data with reasonable security appropriate to the volume and nature of the personal data, and considering the controller's size and type.

Controllers are prohibited from processing sensitive data without providing the consumer with a right to opt-out. Under the UCPA, sensitive data includes any personal data that reveals a consumer's racial or ethnic origin, religious beliefs, sexual orientation, or citizenship or immigration status, as well as certain health care-related data, biometric data, and specific geolocation data. Similarly, consumers cannot be discriminated against, in the form of denial of service, different pricing, or diminished quality of service, for exercising any of their rights under the UCPA.[12]

Processor Obligations

The UCPA requires processors and controllers to enter into data processing agreements ("DPAs") that specify the instructions, nature, types of data, length, and rights and obligations subject to processing.[13] Processors are subject to confidentiality requirements for their personnel who handle the data. Further, processors are required to push down the controllers data processing expectations to any subcontractor involved in the processing of the data.

Enforcement

Although the UCPA does not provide a private right of action,[14] the UCPA has included a dual means of enforcement whereby either the Division of Consumer Protection or the Attorney General (if referred) may enforce the law.[15] If the Attorney General decides to take action, the controller or processor will have 30 days from the time of notice to cure the violation and provide written confirmation that (i) the violation has been cured and (ii) there will be no future violation of the cured violation. For uncured violations or where a past violation reoccurs, the Attorney General can initiate an action for actual damages to the consumer and fines up to $7,500 per violation.

Takeaways

With a compliance date of December 31, 2023, the UCPA requires businesses to take action now.

- Determine whether your business is subject to the UCPA as a controller, and consider the availability of the various exemptions.
  - Does the business:
    - conduct business in Utah, or produce products or services targeted to consumers (i.e., Utah residents other than in an employment or commercial context);
    - have annual revenue of at least $25 million; and
    - either:
      - control or processes personal data of at least 100,000 consumers; or
      - derive more than 50 percent of its gross revenue from the sale of personal data and controls or processes the personal data of at least 25,000 consumers?
  - Do exemptions apply to either the entity or the data, such as for entities regulated under HIPAA or the GLBA, and for data collected in the B2B or employment contexts?
- If the UCPA applies, and to the extent that exemptions are not available:
  - Identify how compliance with UCPA intersects with pre-established compliance programs for CCPA, VCDPA, CPA, and/or the European Union's General Data Protection Regulation ("GDPR") to leverage the compliance effort.
- Review and update your organization privacy notices and vendor data processing agreements to ensure that the requirements of the UCPA will be satisfied by December 31, 2023.

***

[1] S.B. 227, § 13-61-101(12).

[2] *Id*. § 13-61-101(26)

[3] § 13-61-102

[4] § 13-61-101(10)(a), (b).

[5] *Id*.

[6] *Id*.

[7] *Id*. at § 13-61-201; *see also* C.R.S. §6-1-1301, et seq.; Va. Code Ann. § 59.1-571, et seq.;Cal. Civ. Code § 1798.100, et seq.

[8] § 13-61-202.

[9] § 13-61-203.

[10] *Id*.

[11] § 13-61-302.

[12] *Id*.

[13] § 13-61-301.

[14] § 13-61-305.

[15] §§ 13-61-401, 402.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber