# Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

## Utah Consumer Privacy Act: What Businesses Need to Know

April 8, 2022

With the recent signing of the Utah Consumer Privacy Act (UCPA) by Gov. Spencer J. Cox on March 24, 2022, Utah has become the fourth state to enact a comprehensive law addressing consumer data privacy, joining California, Colorado and Virginia. Similar to other comprehensive privacy laws, the UCPA gives companies doing business in the state nearly two years to comply, taking effect on December 31, 2023.

The UCPA bears a greater resemblance to the Virginia Consumer Data Protection Act (VCDPA) than to the California Consumer Privacy Act (CCPA) or the Colorado Privacy Act (CPA), and is more business-friendly than all three. You can read more about the specifics of each of these laws in our previous posts here and here.

Below we provide details on key provisions of the UCPA and highlight how it is different than other comprehensive privacy laws.

### Who Must Comply with the UCPA?

Like the VCDPA, CPA and the General Data Protection Regulation (GDPR), the UCPA applies to "controllers" and "processors." A controller is defined under the UCPA as "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] while a processor is "a person who processes personal data on behalf of a controller."[2]

The UCPA applies to controllers and processors that conduct business in Utah or produce products or services targeted to Utah residents, have an annual revenue of $25,000,000 or more, and either:

- Control or process the personal data of 100,000 or more consumers annually.
- Derive over 50 percent of their gross revenue from the sale of personal data and control or process the personal data of 25,000 or more consumers.[3]

This applicability is narrower than other state privacy laws, adopting a revenue threshold that is not found in the CPA or the VCDPA, but that we have seen in broader form in the CCPA and the amendments made to it by the California Privacy Rights Act (CPRA).[4]


**Contact Information**

**Natasha G. Kohne**
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

**Michelle A. Reed**
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

**Jo-Ellyn Sakowitz Klein**
Senior Counsel
jsklein@akingump.com
Washington, D.C.
+1 202.887.4220

**Rachel Claire Kurzweil**
Counsel
rkurzweil@akingump.com
Washington, D.C.
+1 202.887.4253

**Lauren E. York**
Counsel
lyork@akingump.com
Dallas
+1 214.969.4395

**Tina M. Jeffcoat**
Associate
cjeffcoat@akingump.com
Dallas
+1 214.969.2741

**Dylan L. Moore**
Associate
moored@akingump.com
Dallas
+1 214.969.2758

## Which Entities and Data Are Exempt?

The UCPA includes both data-specific and entity-level exemptions. Data categories that are exempt include data subject to specified federal laws, such as protected health information (as defined under HIPAA,[5] PHI[6]), data collected, processed, sold or disclosed in accordance with the Gramm-Leach-Bliley Act (GLBA), as well as data regulated by the Fair Credit Reporting Act (FCRA), the Driver's Privacy Protection Act (DPPA), the Farm Credit Act (FCA) and the Family Educational Rights and Privacy Act (FERPA).[7] Like the VCDPA, the UCPA exempts data processed or maintained (1) in the course of an individual applying to, or acting as an employee, agent or independent contractor of a controller, processor or third party, to the extent that the data is collected and used within the context of that role; (2) as emergency contact information for an individual and used for emergency contact purposes; or (3) to administer benefits for another individual and used to administer those benefits.[8] Similarly, a controller is compliant with any obligation to obtain parental consent if it complies with the requirements of the Children's Online Privacy Protection Act (COPPA).[9]

In addition to these data-based exemptions, the UCPA contains a number of entity-level exemptions. The UCPA does not apply to entities such as nonprofits, financial institutions or affiliates of financial institutions governed by the GLBA, institutions of higher education, "covered entities" and "business associates" as defined under HIPAA,[10] government entities or third-party contractors acting on their behalf, tribes, air carriers, or to personal data that is processed purely for personal or household purposes.[11]

Notably, the Utah law has data-based exemptions relevant to the health and life sciences sector that are quite broad and explicitly defined, particularly as compared to those available under the CCPA. The UCPA includes an extensive list of health-related information that is exempt, beyond PHI, including (1) information that has been de-identified in accordance with HIPAA;[12] (2) patient identifying information as defined under the Confidentiality of Substance Use Disorder Patient Records regulations (commonly known as "Part 2");[13] (3) a broad swath of information collected in the course of conducting clinical research;[14] and (4) information originating from, and intermingled to be indistinguishable with, PHI or certain other exempt information that is maintained by a health care facility or health care provider[15] or by a program or qualified service organization under Part 2.[16] Not all health information, however, is outside the scope of the UCPA. Non-exempt personal data that reveals information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional, along with certain genetic personal data or biometric data, may be considered "sensitive data" and afforded additional protections, as described below.[17]

## What Is "Personal Data" Under the UCPA?

Similar to the other comprehensive state privacy laws, personal data under the UCPA is defined as "information that is linked or reasonably linkable to an identified or identifiable individual."[18] This does not include deidentified, aggregated or publicly available information.[19] The UCPA mandates that covered businesses controlling or processing consumers' personal data must safeguard that data and provide clear information to consumers about how the data is used. Much like the VCDPA and CPA,

"consumer" is defined as an "individual who is a resident of the state acting in an individual or household context," but does not include individuals acting in an employment or commercial capacity.[20]

The UCPA also provides a definition for "sensitive data," but unlike the VCDPA and the CPA, it **does not** require consumer consent for processing such data. The UCPA defines "sensitive data" as personal data that reveals an individual's (1) racial or ethnic origin; (2) religious beliefs; (3) sexual orientation; (4) citizenship or immigration status; or (5) medical history, mental or physical health, medical treatment or diagnosis by a health care professional, plus specific geolocation data and certain genetic personal data or biometric data, all subject to limited exceptions. The UCPA requires that businesses provide notice and an opportunity to opt out of the use of this sensitive data.[21] Under the UCPA consent is only required in the context of parental consent for processing children's data.[22]

## What Rights Do Utah Consumers Have?

While the UCPA provides similar consumer privacy rights to the other state privacy laws, there are certain key differences. For example, a consumer only has the right to delete personal data that they provide to the controller. Additionally, the UCPA does not provide a right for consumers to appeal denials of requests to exercise their rights, correct personal data or to opt out of profiling.

The UCPA grants consumers the right to (1) access and confirm whether a controller is processing their personal data; (2) delete personal data that they provided to the controller; (3) obtain a copy of their personal data provided to the controller to the extent it is feasible, portable, practical and usable while allowing the consumer to transmit the data to another controller; and (4) opt out of processing for the purposes of targeted advertising or the sale of personal data.[23] Controllers must respond to consumer requests within 45 days of receipt, with an additional 45 day extension available in complex or high-volume cases provided that the controller informs the consumer of the reason for the extension and the extension is reasonably necessary.[24]

## What Constitutes a "Sale" Under the UCPA?

The UCPA defines a sale of personal information as "the exchange of personal data for monetary consideration by a controller to a third party."[25] This differs from the CCPA and CPA, which include "other valuable consideration" in the definition of a "sale."[26] Unlike in California, Colorado or Virginia, the UCPA's definition of a sale contains a unique exemption that allows a controller to disclose personal data to a third party if the purpose is consistent with the consumer's "reasonable expectations."[27]

Activities that do not constitute a sale under the UCPA include (1) a controller's disclosure of personal data to a processor who processes it on behalf of the controller; (2) disclosures of personal data from a controller to its affiliate; (3) the disclosure or transfer of personal data when a consumer directs the controller to disclose it or interact with third parties; (4) a controller's disclosure of personal data to a third party if the purpose is consistent with the consumer's reasonable expectations (considering the context in which the consumer provided the data); (5) a consumer's disclosure of personal data to a third party in order to provide a product or service requested by

either the consumer or a parent/legal guardian of a child; (6) disclosures of information when a consumer intentionally makes it available to the general public via mass media and does not restrict it to a specific audience; and (7) a controller's transfer of personal data to a third party as part of an asset for a merger, acquisition or bankruptcy in which the third party assumes control of the controller's assets.[28]

## What Obligations Do Controllers and Processors Have?

The UCPA contains requirements for both controllers and processors. These requirements are largely the same as those found in the CPA and VCDPA, with some differences. Processors are required to (1) adhere to controller instructions; and (2) taking into account the nature of the processing and information available to the processor, use appropriate technical and organizational measures to assist the controller in meeting its obligations, including obligations related to security and notification of a data breach. Controllers and processor must also enter into a contract that (a) sets out the controller's instructions for processor personal data, the nature and purpose of the processing, the type of data, the duration of the processing, and the parties rights and obligations; and (b) requires the processor to (i) ensure each person processing the personal data is subject to a duty of confidentiality; (ii) ensure each subcontractor is under a written contract subjecting them to the same obligations as the processor.[29] Unlike the CPA and VCDPA, there is no requirement that processors allow for audits or inspections by controllers or designated auditors of controllers.

Controller obligations under the UCPA are as follows:

- ***Transparency and purpose specification***: A controller must provide a reasonably clear and accessible privacy notice to consumers that includes (1) the categories of personal data processed by the controller; (2) the purposes for which those categories are processed; (3) how consumers may exercise a right; (4) any categories of personal data that the controller shares with third parties; and (5) the categories of any third parties with whom the controller shares personal data.[30] Additionally, if a controller "sells" a consumer's personal data to one or more third parties, or engages in targeted advertising, the controller must clearly and conspicuously disclose how a consumer can exercise their right to opt out of the sale or processing for targeted advertising.[31]
- ***Sensitive data***: As previously mentioned, the UCPA does not require opt-in consent for processing sensitive data. Instead, controllers must provide consumers with notice and an opportunity to opt out before processing sensitive data. In the case of personal data concerning a child, controllers must process the data in accordance with the COPPA.[32]
- ***Security***: Controllers must establish and maintain reasonable administrative, technical and physical data security practices. These practices must guard the confidentially and integrity of personal data while reducing reasonably foreseeable risks to consumers relating to the processing. A controller must take into account the size, scope and type of its business to implement data security that is appropriate for the volume and nature of the data it collects.[33]
- ***Nondiscrimination***: A controller cannot deny a good or service, charge a different price or provide a different level of quality to a consumer that exercises their rights

under the UCPA. However, controllers are still permitted to offer different prices or discounts if the consumer has opted out of targeted advertising or if the offer is related to the consumer voluntarily participating in a loyalty program.[34]

- ***Provision of Products and Services***: A controller is not required to provide a product, service or functionality to a consumer if the consumer's personal data is reasonably necessary for the controller to provide that product, service or functionality, and the consumer did not provide the personal data or allow the controller to process their personal data.[35]

Unlike the VCDPA and CPA, the UCPA does not include any requirement for data protection assessments or to conduct cybersecurity audits or risk assessments.

## Who Enforces the UCPA?

Enforcement is one of the most distinctive aspects of the UCPA. The UCPA **does not** include a private right of action. While the Utah Attorney General (AG) has exclusive power to enforce the UCPA, the Utah Department of Commerce Division of Consumer Protection (the "Division") is tasked with receiving and investigating consumer complaints.[36] When the director of the Division determines there is "reasonable cause to believe that substantial evidence exists" that a business is in violation of the UCPA, the director will refer the matter to the AG. Prior to initiating any enforcement action, the AG will provide notice of the violation to the controller or processor with a 30-day cure period that **does not** sunset, unlike the cure period for the Colorado privacy law.[37] The AG can recover actual damages to the consumer and up to $7,500 per incident, much like the VCDPA.[38]

Additionally, the UCPA requires the AG and the Division to compile and submit an enforcement report to the Business and Labor Interim Committee by July 1, 2025. The report must evaluate the liability and enforcement provisions of the UCPA, including the effectiveness of enforcement efforts, and summarize the data protected and not protected by the law.[39]

## Key Takeaways

The UCPA is arguably the most business friendly comprehensive privacy legislation passed in the United States to date. It creates many of the same obligations imposed by California, Colorado and Virginia, but provides a laundry list of exemptions for companies already regulated by certain statutory privacy regimes. Generally, the UCPA bears more resemblance to Virginia's law than Colorado's, adopting, for example, the VCDPA's narrower definition of "sale" and providing enforcement exclusively through the state attorney general. The UCPA is unique in that it excludes certain provisions such as opt-in consent, opt-out for profiling and required data processing assessments for controllers, while adding unique features such as disclosure to third parties when the purpose is consistent with a consumer's reasonable expectations. Moreover, the UCPA has a distinctive enforcement mechanism—requiring Division investigation prior to AG enforcement is a significant part of what makes the UCPA even more business friendly than other comprehensive privacy laws. We recommend that companies assess whether they are covered by the UCPA and develop a plan for compliance before the law goes into effect on December 31, 2023.

[1] S.B. 227 § 13-61-101(12).

[2] *Id.* § 13-61-101(26).

[3] *Id.* § 13-61-102(1).

[4] Cal. Civ. Code § 1798.140(d). The CPRA applies to businesses that conduct business in California and satisfy one or more of the following thresholds: (1) annual gross revenue in excess of $25,000,000 in the preceding year; (2) annually buys, sells or shares personal information of 100,000 or more consumers or households; or (3) derives 50 percent or more of its annual revenue from selling or sharing consumers' personal information.

[5] "HIPAA" refers to the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, and their implementing regulations (codified at 45 C.F.R. parts 160 and 164).

[6] S.B. 227 § 13-61-102(2)(g)(i).

[7] *Id.* § 13-61-102(2).

[8] *Id.* § 13-61-102(2)(o).

[9] *Id.* § 13-61-102(3).

[10] 45 C.F.R. § 160.103. A "covered entity" is a health plan, a health plan clearinghouse, or a health care provider (like a hospital, nursing home, or outpatient clinic) that engages in standard HIPAA transactions, like electronic billing. "Business associate" is defined to include a person (other than a member of a covered entity's workforce) or entity that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of PHI.

[11] S.B. 227 § 13-61-102(2).

[12] 45 C.F.R. § 164.514(a)-(c); S.B. 227 § 13-61-102(2)(g)(ix).

[13] 42 C.F.R. Part 2; S.B. 227 § 13-61-102(2)(g)(ii).

[14] S.B. 227 § 13-61-102(2)(g)(iii)-(v).

[15] Note that "health care facility" and "health care provider" are defined under the UCPA to reference state law meanings. *See id.* § 13-61-101(18)-(19).

[16] *Id.* § 13-61-102(2)(h).

[17] *Id.* § 13-61-101(32).

[18] *Id.* § 13-61-101(24)(a).

[19] *Id.* § 13-61-101(24)(b).

[20] *Id.* § 13-61-101(10).

[21] *Id.* § 13-61-302(3).

[22] *Id.* § 13-61-302(3)(b).

[23] *Id.* § 13-61-201(1)-(4).

[24] *Id.* § 13-61-203(2).

[25] *Id.* § 13-61-101(31)(a).

[26] C.R.S. § 6-1-1303(23)(a) (noting that under the CPA, a sale means "the exchange of personal data for monetary or other valuable consideration by a controller to a third party").

[27] S.B. 227 § 13-61-101(31)(b)(iii).

[28] *Id.* § 13-61-101(b).

[29] *Id.* § 13-61-301(1)-(3).

[30] *Id.* § 13-61-302(1).

[31] *Id.* § 13-61-302(1)(b).

[32] *Id.* § 13-61-302(3).

[33] *Id.* § 13-61-302(2).

[34] *Id.* § 13-61-302(4).

[35] *Id.* § 13-61-302(5).

[36] *Id.* § 13-61-401(1)-(2).

[37] *Id.* § 13-61-402(3)(a)-(b); C.R.S. § 6-1-1311(1)(d).

[38] S.B. 227 § 13-61-402(3)(d).

[39] *Id.* § 13-61-404.