Computer & Communications Industry Association
Tech Advocacy Since 1972

Utah's "Consumer Privacy Act" Summary

On March 24, 2022, Governor Cox signed SB227, the "Consumer Privacy Act" ('UCPA') into law. The Act's provisions take effect on December 31, 2023. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	• The UCPA applies to any controller or processor who conducts business in the state **or** produces a product or service that is targeted to consumers who are residents of the state; **and** has annual revenue of $25,000,000 or more; **and** satisfies one or more of the following thresholds: (1) during a calendar year, controls or processes personal data of 100,000 or more consumers; **or** (2) 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.
Covered Data	• "**Personal data"** means information that is linked or reasonably linkable to an identified individual or an identifiable individual. Personal data does not include de-identified data, aggregated data, or publicly available information. • **"Sensitive data"** means personal data that reveals (a) an individual's racial or ethnic origin; (b) an individual's religious beliefs; (c) an individual's sexual orientation; (d) an individual's citizenship or immigration status; or (e) information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional. Sensitive data also includes the processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual; or specific geolocation data.
Key Definitions	• ***"Consent"***: an affirmative act by a consumer that unambiguously indicates the consumer's voluntary and informed agreement to allow a person to process personal data related to the consumer. • ***"De-identified Data"***: data that cannot reasonably be linked to an identified individual or an identifiable individual and are possessed by a controller who (a) takes reasonable measure to ensure that a person cannot associate the data with an individual; (b) publicly commits to maintain and use the data only in de-identified form and not attempt to re-identify the data; and (c) contractually obligates any recipients of the data to comply with the requirements. • ***"Pseudonymous Data"***: personal data that cannot be attributed to a specific individual without the use of additional information, if the additional information is (a) kept separate from the consumer's personal data; and (b) subject to appropriate technical and organizational measures to ensure that the personal data are not attributable to an identified individual or an identifiable individual. • ***"Sale"***: the exchange of personal data for monetary consideration by a controller to a third party. A sale does not include: (1) a controller's disclosure of personal data to a processor who processes the personal data on behalf of the controller; (2) a controller's disclosure of personal data to an affiliate of the controller; (3) considering the context in which the consumer provided the personal data to the controller, a controller's disclosure of personal data to a third party if the purpose is consistent with a consumer's reasonable expectations; (4) the disclosure or transfer of personal data when a consumer directs a controller to disclose the personal data or interact with one or more third parties; (5) a consumer's disclosure of personal data to a third party for the purpose of providing a product or service requested by the consumer or a parent or legal guardian of a child; (6) the disclosure of information that the consumer intentionally makes available to the general public via a channel of mass media and does not restrict to a specific audience; or (7) a controller's transfer of personal data to a third party as an asset that is part of a proposed or actual merger, an acquisition, or a bankruptcy in which the third party assumes control of all of part of the controller's assets. • ***"Targeted Advertising"***: displaying an advertisement to a consumer where the advertisement is selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.
Consumer Rights	• **Affirmative Consent**: A controller may not process sensitive data collected from a consumer without (a) first presenting the consumer with clear notice and an opportunity to opt out of the processing; or (b) in the case of processing of personal data concerning a known child, processing the data in accordance with COPPA. • **Access**: A consumer has the right to confirm whether a controller is processing the consumer's personal data and access the consumer's personal data. • **Deletion**: A consumer has the right to delete the consumer's personal data that the consumer provided to the controller. • **Portability**: A consumer has the right to obtain a copy of the consumer's personal data, that the consumer

	previously provided to the controller in a format that (1) to the extent technically feasible, is portable; (2) to the extent practicable, is readily usable; and (3) allows the consumer to transmit the data to another controller without impediment, where the processing is carried out by automated means. • **Opt Out Rights**: A consumer has the right to opt out of the processing of the consumer's personal data for purposes of targeted advertising or; the sale of personal data.
Business Obligations	• **Transparency / Purpose Specification:** A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes (1) the categories of personal data processed by the controller; (2) the purposes for which the categories of personal data are processed; (3) how consumers may exercise a right; (4) the categories of personal data that the controller shares with third parties, if any; and (5) the categories of third parties, if any, with whom the controller shares personal data. • **Security:** A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to protect the confidentiality and integrity of personal data and reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data. • **Avoid Unlawful Discrimination:** A controller may not discriminate against a consumer for exercising a right in this Act by denying a good or service to the consumer, charging the consumer a different price or rate for a good or service, or providing the consumer a different level of quality of a good or service. • **Responding to Consumer Request:** A controller shall comply with a consumer's request to exercise a right within 45 days (may be extended by an additional 45 days if reasonably necessary) after the day on which a controller receives a request to exercise a right. A controller may not charge a fee for information in response to a request unless the request is the consumer's second or subsequent request during the same 12-month period or is excessive, repetitive, technically infeasible, or manifestly unfounded.
Data Protection Assessment	• **The Attorney General shall compile a report** evaluating the liability and enforcement of the UCPA and summarizing the data protected and not protected with a list of the types of information that are publicly available from local, state, and federal government sources.
Controller / Processor Distinction	• **A processor shall adhere to the controller's instructions** and take into account the nature of the processing and information available to the processor 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. • Before a processor performs processing on behalf of a controller, the processor and controller shall enter into a contract that (1) 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' right and obligations; (2) requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data; and (3) 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.
Exceptions	• The **UCPA contains exceptions for the processing of de-identified data and pseudonymous data**. • The UCPA does not restrict a controller's or processor's ability to: (a) comply with laws; (b) comply with inquiries by government entities; (c) cooperate in good faith with the enforcement agency; (d) investigate and defend a legal claim; (e) provide a product of service requested by a consumer; (f) perform a contract; (g) take immediate steps to protect an interest essential for the life and safety of the consumer; (h) detect or prevent illegal activity; (i) engage in public or peer-reviewed scientific research; (j) assist another person with an obligation in the UCPA; (k) process personal data; (l) retain a consumer's email address to comply with the consumer's request. • Data exempt from the UCPA includes protected information under HIPAA, the Federal Policy for the Protection of Human Subjects, the Health Care Quality Improvement Act of 1986, the Fair Credit Reporting Act, GLBA, FERPA, the Farm Credit Act of 1971, and COPPA.
Enforcement	• The UCPA **preempts local laws** and **does not provide a basis for, nor is a violation of the UCPA subject to, a private right of action**. • The **Attorney General has the exclusive authority to enforce the UCPA** and must provide written notice at least 30 days before an initiation of an enforcement action. The **Consumer Privacy Account** is funded by money received through civil enforcement actions under the UCPA to be used to support investigating violations of the Consumer Privacy Account.