Computer & Communications
Industry Association
Tech Advocacy Since 1972

Connecticut’s “An Act Concerning Personal Data Privacy and Online Monitoring,” Summary

On May 10, 2022, Governor Lamont signed SB6, “An Act Concerning Personal Data Privacy and Online Monitoring” (‘CTDPA’), into law. The majority of the Act takes effect on July 1, 2023. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	• The CTDPA applies to persons that conduct business in this state or persons that produce products or services that are **targeted** to residents of this state and that during the preceding calendar year (1) controlled or processed the personal data of not less than 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; **or** (2) controlled or processed the personal data of not less than 25,000 consumers and derived more than 25% of their gross revenue from the sale of personal data.
Covered Data	• “**Personal data**” means any information that is linked or reasonably linkable to an identified or identifiable individual and does not include de-identified data or publicly available information. • **“Sensitive data”** means personal data that includes (a) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status; (b) the processing of genetic or biometric data for the purpose of uniquely identifying an individual; (c) personal data collected from a known child, or (d) precise geolocation data.
Key Definitions	• ***“Consent”***: a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. Consent does not include (a) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; (b) hovering over, muting, pausing or closing a given piece of content; or (c) agreement obtained through the use of dark patterns. • ***"Dark pattern"***: a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and includes, but is not limited to, any practice the FTC calls a dark pattern. • ***"De-identified data"***: data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual. • ***"Pseudonymous data"***: personal data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual. • ***"Sale"***: the exchange of personal data for monetary or other valuable consideration by the controller to a third party. • ***"Targeted advertising"***: displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests.
Consumer Rights	• **Access**: A consumer shall have the right to confirm whether or not a controller is processing the consumer's personal data and access such personal data, **unless access would require the controller to reveal a trade secret**. • **Correction**: A consumer shall have the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data. • **Deletion**: A consumer shall have the right to delete personal data provided by, or obtained about, the consumer. • **Portability**: A consumer shall have the right to obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret • **Opt Out Rights**: A consumer shall have the right to opt out of the processing of the personal data for purposes of (a) targeted advertising; (b) the sale of personal data; or (c) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. • **Affirmative Consent:** A controller shall not process sensitive data concerning a consumer without obtaining the consumer's consent, or without processing such data in accordance with COPPA in the case of a known child.

Business Obligations	● **Responding to consumer request:** A controller shall respond to the consumer without undue delay, but not later than 45 days after receipt of the request (may be extended by 45 additional days when reasonably necessary). Information provided shall be free of charge once per consumer during a 12-month period unless manifestly unfounded, excessive, or repetitive. Within 60 days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal. If the appeal is denied, the controller shall also provide the consumer with an online mechanism to contact the Attorney General to submit a complaint. ● **Data minimization:** A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. ● **Purpose specification:** A controller shall not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent. ● **Security:** A controller shall establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue. ● **Avoid unlawful discrimination:** A controller shall not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers. ● **Avoid secondary use:** A controller shall not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge, and wilfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age. ● **Responding to consumer revocation:** A controller shall provide an effective mechanism for a consumer to revoke the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request. ● **Transparency:** A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes (1) the categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights; (4) the categories of personal data that the controller shares with third parties; (5) the categories of third parties with which the controller shares personal data; and (6) an active electronic mail address that the consumer may use to contact the controller.
Data Protection Assessments	● **A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer**. The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the AG.
Controller / Processor Distinction	● **A processor shall adhere to the instructions of a controller** and assist the controller in meeting the controller's obligations of this Act. A contract between a controller and a processor shall govern the processor's data processing procedures and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, and the duration of processing and the rights and obligations of both parties.
Exceptions	● **The CTDPA contains exceptions for the processing of de-identified data and pseudonymous data**. The CTDPA shall not be construed to restrict a controller's or processor's ability to: (a) comply with regulations; (b) comply with regulatory inquiries; (c) cooperate with law enforcement in good faith; (d) investigate or defend legal claims; (e) provide a product or service specifically requested by a consumer; (f) perform under a contract to which a consumer is a party; (g) take steps at the request of a consumer prior to entering into a contract; (h) take immediate steps to protect an interest essential for the life or safety of the consumer; (i) prevent or respond to security incidents; (j) engage in peer-reviewed scientific or statistical research in the public interest; (k) assist another controller with the obligations under this Act; or (l) process personal data for reasons of public interest. ● Data exempt from the CTDPA includes protected information under HIPAA, the Federal Policy for the Protection of Human Subjects, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, and the Airline Deregulation Act.
Enforcement	● The CTDPA does **not provide the basis for a private right of action** for violations. The **Attorney General shall**

	have exclusive authority to enforce violations of this Act. Beginning on July 1, 2023, the Attorney General shall issue a notice of violation to the controller if the Attorney General determines that a cure is possible. Beginning on January 1, 2025, the Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation consider: (1) the number of violations; (2) the size and complexity of the controller or processor; (3) the nature and extent of the processing activities; (4) the substantial likelihood of injury to the public; (5) the safety of persons or property; and (6) whether such violation was likely caused by human or technical error. ● Not later than September 1, 2022, the chairpersons of the joint standing committee of the General Assembly having cognizance of matters relating to general law **shall convene a task force to study topics concerning data privacy**.