Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

# Connecticut Data Privacy Act—What Businesses Need to Know

May 26, 2022

The Connecticut Data Privacy Act (CTDPA), which will go into effect July 1, 2023, is now the fifth and latest comprehensive state consumer privacy law, giving companies doing business in the state less than two years to comply.

The CTDPA has many similarities with other states (California, Virginia, Colorado and Utah) that have passed consumer privacy laws, but is most similar to the Virginia Consumer Data Privacy Act (VCDPA) and the Colorado Privacy Act (CPA), which are more consumer-oriented than the more business-friendly Utah Consumer Privacy Act (UCPA) (more on the UCPA here).

All of these state consumer privacy laws, including the California Consumer Privacy Act (CCPA), involve multiple detailed consumer rights and company obligations that compliance plans will need to account for (see our previous posts here and here). Below, we provide an overview of the new law, comparing and contrasting it to the other operative consumer privacy regimes.

## Who Must Comply with the CTDPA?

Just as with the VCDPA, CPA, UCPA and Europe’s General Data Protection Regulation (GDPR), the CTDPA applies to data “controllers” and “processors.” A “controller” under the CTDPA refers to “an individual who, or legal entity that, alone or jointly with others determines the purposes and means of processing personal data,”[1] while processor refers to “an individual who, or legal entity that, processes personal data on behalf of a controller.”[2]

The CTDPA applies to persons conducting business in Connecticut or producing products or services targeted to Connecticut residents, and who during the preceding calendar year either:

- Controlled or processed the personal data of 100,000 or more consumers annually, except for personal data controlled or processed solely for the purpose of completing a payment transaction.
- Derived over 25 percent of their gross revenue from the sale of personal data and controlled or processed the personal data of 25,000 or more consumers.[3]

**Contact Information**

**If you have any questions concerning this alert, please contact:**

**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

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

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

**Charles (Chase) Hamilton**
Associate
hamiltonc@akingump.com
Dallas
+1 214.969.2856

Similar to the VCDPA and the CPA, the CTDPA does not contain a revenue threshold. Thus, unlike the CCPA (as amended by the California Privacy Rights Act (CPRA)) or UCPA, an entity will not become subject to the law due to its annual revenues or by exceeding a certain revenue requirement.[4] However, the CTDPA's 25 percent gross revenue obtained from data sales threshold is a substantial difference from the 50 percent gross revenue limit found in the VCDPA and UCPA.  Thus, more companies are likely to find themselves covered by the Connecticut law.

## Which Entities and Data Are Exempt?

Like other consumer privacy laws, the CTDPA contains both entity-level and data-based exemptions, including a number of exemptions concerning health and life sciences data.

*Entity-level exemptions*: The CTDPA exempts state and local government entities, nonprofits, institutions of higher education, certain national security associations, financial institutions covered by the Gramm-Leach-Bliley Act (GLBA) and "covered entities" and "business associates" as defined under HIPAA.[5]

*Data-based exemptions*: Data exempt under the CTDPA includes personal data regulated by the Fair Credit Reporting Act (FCRA), the Driver's Privacy Protection Act (DPPA), the Family Educational Rights and Privacy Act (FERPA), the Farm Credit Act (FCA) and the Airline Deregulation Act (ADA).[6] Like the VCDPA and the UCPA, the CTDPA 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.[7] Additionally, similar to the VCDPA and UCPA, there is a limited exemption for processing children's data. Specifically, controllers and processors that comply with the requirements of the Children's Online Privacy Protection Act (COPPA) are compliant with any parental consent requirements of the CTDPA.[8]

*Health and life sciences data exemptions*: In addition to the exemption for HIPAA covered entities and business associates, the CTDPA includes some specific data-based exemptions particularly relevant to the health and life sciences sector. For example, the CTDPA exempts (1) protected health information (PHI) as defined under HIPAA,[9] (2) information derived from certain health care related information that is de-identified in accordance with HIPAA,[10] (3) information used for public health activities and purposes as authorized by HIPAA,[11] (4) patient identifying information for purposes of 42 U.S.C. § 290dd-2, which concerns the confidentiality of substance use disorder patient records (as regulated under "Part 2" – 42 C.F.R. part 2),[12] (5) a range of clinical research information[13] and (6) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, CTDPA-exempt information that is maintained by a covered entity or business associate or by a Part 2 program or qualified service organization.[14]

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

Similar to the other comprehensive state privacy laws, the CTDPA defines personal data as "any information that is linked or reasonably linkable to an identified or

© 2022 Akin Gump Strauss Hauer & Feld LLP

identifiable individual."[15] The law also excludes from the definition de-identified or publicly available information.[16]

Like the VCDPA, the UCPA, and the CPA, the CTDPA's definition of "consumer" specifies that an individual must be a Connecticut resident and explicitly excludes individuals "acting in a commercial or employment context." This means information collected in the context of a business-to-business or employment relationship will not be covered by the CTDPA.[17]

Like the VCDPA and CPA (but unlike the UCPA), the CTDPA requires opt-in consent for the collection and processing of "sensitive data."[18] The CTDPA defines sensitive data as personal data that reveals (1) racial or ethnic origin, (2) religious beliefs, (3) mental or physical health condition or diagnosis, (4) sex life, (5) sexual orientation, (6) citizenship or immigration status, (7) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, (8) children's data and (9) precise geolocation data.[19]

In its definition of "consent," the CTDPA also explicitly excludes dark patterns.[20] Much like other state consumer privacy laws as well as the GDPR, consent under the CTDPA must be "freely given, specific, informed and unambiguous."[21]

## What Rights Do Connecticut Consumers Have?

The CTDPA grants consumers a broad swath of rights. Specifically, the CTDPA grants consumers the right to appeal denials of requests by controllers,[22] along with the CPA's right to opt out of processing for either targeted advertising or sales of personal data.[23]

Similar to other comprehensive privacy laws, the CTDPA grants consumers the following rights:

- **Access**. Consumers have the right to confirm whether a controller is processing their personal data and access such personal data, unless such actions would reveal a trade secret.
- **Correction**. Consumers have the right to correct inaccuracies in their personal data (with some limitation).
- **Deletion**. Consumers have the right to delete personal data provided by or about the consumer.
- **Data portability**. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible and provided the controller will not be required to reveal any trade secret.[24]
- **Opt-out of certain data processing**. Consumers have the right to opt out of the processing of personal data for purposes of (i) targeted advertising, (ii) the sale of personal data or (iii) profiling in connection with automated decisions that produce legal or similarly significant effects concerning the consumer.[25]

As with the CCPA and CPA, the CTDPA also grants consumers the ability to designate another person as an authorized agent to exercise the right to opt out on their behalf.[26]

Similar to the other comprehensive state privacy laws, the CTDPA grants controllers 45 days to respond to consumer requests, extendable once by an additional 45 days as “reasonably necessary,” considering the complexity and number of the consumer’s requests.[27]

## What Constitutes a “Sale” Under the CTDPA?

The CTDPA defines “sale of personal data” as the exchange of personal data for monetary or other valuable consideration by the controller to a third party.[28] Notably, this is similar to the CCPA and CPA, which also include that a sale will occur in exchange for “other valuable consideration.”[29]

Activities that do not constitute a sale under the CTDPA include (1) the disclosure of personal data to a processor that processes the personal data on behalf of the controller, (2) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer, (3) the disclosure or transfer of personal data to an affiliate of the controller, (4) the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party, (5) the disclosure of personal data that the consumer intentionally made available to the general public via a channel of mass media, and did not restrict to a specific audience or (6) the disclosure or transfer of personal data to as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the controller’s assets.[30]

## What Obligations Do Controllers and Processors Have?

The CTDPA contains requirements for both controllers and processors, similar to those found in the other state privacy laws.

*Requirements for Processors*. Processors are required to adhere to controller instructions and assist the controller with its obligations under the CTDPA by “(1) [t]aking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller’s obligation to respond to consumer rights requests; (2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller’s obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as defined in section 36a-701b of the general statutes, of the system of the processor, in order to meet the controller’s obligations; and (3) providing necessary information to enable the controller to conduct and document data protection assessments.”[31]

Additionally, as with the other state privacy laws and the GDPR, the relationship between a controller and processor must be governed by a contract that sets forth the controller’s instructions for processing data, the nature and purpose of the processing, the duration of the processing, and the rights and obligations of both parties. The contract must also require that the processor (1) ensure each person processing the data is subject to a duty of confidentiality with respect to the data, (2) delete or return the personal data at the controller’s discretion unless retention is required by law, (3) make available any information necessary for compliance to the controller, (4) after providing the controller with an opportunity to object, engage any subcontractor with a written contract that requires adherence to the processor’s obligations, and (5) allow and cooperate with reasonable assessments by the controller or the controller's designated assessor.[32]

*Requirements for Controllers*. Controller obligations under the CTDPA are as follows:

- **Transparency and purpose specification**: A controller must provide consumers with a reasonably clear and meaningful privacy notice that includes (1) categories of personal data processed, (2) the purpose for processing the personal data, (3) instructions for consumers to exercise their rights, including how to appeal a rejected consumer request, (4) categories of personal data shared with third parties and (5) the controller's email address or other online contact mechanism.[33] The privacy policy must also contain a description of how consumer may submit consumer rights request.
- **Data minimization**: A controller must limit collection of personal data to what is adequate, relevant and reasonably necessary for the disclosed purposes for which the data is processed.[34]
- **Avoid secondary use**: Unless the controller obtains the consumer's consent, the controller may 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.[35]
- **Security**: Controllers must establish, implement and maintain reasonable administrative, technical and physical security practices to protect the confidentiality, integrity and accessibility of the personal data. These practices must take into account the volume and nature of the personal data in question.[36]
- **Sensitive data**: Like the VCDPA and the CPA, the CTDPA requires a controller to obtain a consumer's opt in consent before processing that consumer's sensitive data. If the consumer is a child, the controller must process in accordance with COPPA.[37]
- **Nondiscrimination**: Controllers are prohibited from processing personal data in violation of state or federal laws prohibiting unlawful discrimination against consumers.[38] Controllers are also prohibited from discriminating against consumers for exercising their rights, but the CTDPA clarifies that if a consumer's decision to opt out of processing conflicts with the consumer's privacy setting or voluntary participation in a rewards program, the controller may provide notice of the conflict and ask the consumer to confirm the privacy setting or participation in the program.[39]
- **Revocable consent**: Controllers must provide consumers with an effective method to revoke consent that is as easy as the method they used to provide the consent. Upon revocation, the controller must cease processing the data "as soon as practicable but no later than 15 days after receipt of the request."[40]
- **Data protection assessment**: As in the VCDPA, CPA and the CPRA amendments, the CTDPA requires controllers to conduct a data protection assessment (DPA) for processing activities the present a "heightened risk of harm to a consumer." This includes (1) processing personal data for targeted advertising, (2) selling personal data, (3) processing sensitive data or (4) processing personal data for profiling where it involves foreseeable risk of (i) unfair or deceptive treatment or unlawful disparate impact on consumers, (ii) financial, physical or reputational injury to consumer, (iii) intrusion upon the solitude or seclusion, or private affairs of

© 2022 Akin Gump Strauss Hauer & Feld LLP

consumers, or (iv) other substantial injury to consumer.[41] These DPAs must identify and weigh the risks and benefits of the processing to consumers, the controller, other stakeholders and the public at large.[42]

Mirroring the CPA and VCDPA, controllers under the CTDPA must provide DPAs to the Connecticut Attorney General (AG) when required for investigations, which the AG may then evaluate for compliance.[43] As in the CPA, these DPAs are required for data processing created or generated after July 1, 2023, and as in both the CPA and VCDPA, the DPAs are not retroactive.[44] Fortunately for compliance efforts, the CTDPA permits the use of a DPA conducted to satisfy another law if that DPA is "reasonably similar" in scope and effect to what the CTDPA requires.[45]

In a measure similar to the CPRA amendments, controllers under the CTDPA may not process personal data for targeted advertising, or sell a consumer's personal data without consent, when the controller "has actual knowledge, and willfully disregards" that a consumer is between 13 and 15 years of age.[46]

## How are Opt-outs Managed?

If a controller "sells" personal data to a third party or processes personal data for targeted advertising, the CTDPA requires controllers to provide a "clear and conspicuous link" on the controller's website to enable a consumer or that consumer's agent to opt out of targeted advertising or sale of the consumer's personal data.[47] While the CTDPA does not prescribe the label of the link, this clear and conspicuous link is similar to the "Do Not Sell or Share My Personal Information" link required by the CCPA/CPRA. Neither the VCDPA nor the CPA specify the exact manner in which a controller must provide the opt-out right, only that the manner must be "clearly and conspicuously" disclosed by the controller.

Starting on January 1, 2025, controllers must allow consumers the option to opt out of targeted advertising and the sale of personal data through an "opt-out preference signal," sent with consumer consent via a platform, technology or mechanism. The CTDPA requires that this opt out signal must (1) rely on consumers' affirmative unambiguous choice rather than a default setting, (2) not unfairly disadvantage another controller, (3) be consumer-friendly and easy to use, (4) be as consistent as possible with other similar mechanisms required by other laws and (5) enable the controller to accurately determine if a consumer is a resident of the state making a legitimate opt out request.[48]

## Who Enforces the CTDPA?

Similar to most other state consumer privacy laws, the CTDPA does not provide a private right of action. The AG has exclusive enforcement authority, with violations constituting unfair trade practices under the Connecticut Unfair Trade Practices Act (CUTPA).[49] In a move reminiscent of the CPA sunset provision, before pursuing any action for violations, the AG will provide companies with a notice of alleged violations and a 60-day cure period if a cure is possible, from July 1, 2023, until December 31, 2024.[50] The AG has until February 1, 2024, to submit a report to the Connecticut General Assembly on how many notices of violations were given, the nature of each violation, the amount cured and any other matter the AG deems relevant. Beginning January 1, 2025, the AG will be able to grant opportunities to cure alleged violations at the AG's discretion, considering the following factors: (1) the number of violations, (2) the controller or processor's size and complexity, (3) the nature and extent of the processing, (4) the substantial likelihood of injury to the public, (5) the safety of persons or property and (6) whether the alleged violation was caused by a human or technical error.[51]

Additionally, starting September 1, 2022, the Connecticut General Assembly will convene a task force to study a variety of data privacy topics, including (1) information sharing among health care and social care providers, to make recommendations aimed at eliminating health disparities and inequities across sectors, (2) algorithmic decision-making and recommendations to reduce related bias, (3) the possibility of legislation on complying with parent deletion requests under COPPA, (4) age verification of children on social media, (5) data colocation issues, (6) possible expansion of CTDPA and (7) other data privacy topics.[52] This task force has until January 1, 2023, to submit its findings and recommendations.[53]

## Key Takeaways

The CTDPA contains provisions granting similar rights to consumers, placing obligations on data controllers and processors, and providing exemptions to those obligations as the consumer privacy laws of California, Colorado, Virginia and Utah. Overall, the CTDPA has more similarities to Colorado's CPA than Virginia's VCDPA, adopting the Colorado data portability requirement as well as a similar sunset provision and definition of "sale of personal data." The CTDPA has comparatively less in common with the CCPA and the UCPA.

California remains the only state to grant consumers a private right of action. The CTDPA is still much stricter than the UCPA, which was notably more business friendly than other state consumer privacy laws. Companies under the CTDPA will have to honor browser privacy signals, such as the Global Privacy Control, and provide a clear and conspicuous opt out link for consumers on their websites. Significantly, the CTDPA's sunset provision on the right to cure means that starting January 1, 2025, the AG will no longer have to issue notice and an opportunity to cure before pursuing violations, much like the cure period for Colorado.

We recommend that companies assess whether they are covered by the CTDPA and develop a plan for compliance before the law goes into effect on July 1, 2023.

[1] P.A. 22-15 § 1(8).

[2] *Id.* § 1(21).

[3] *Id.* § 2(1)–(2).

[4] Cal. Civ. Code § 1798.140(d). The CCPA 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; S.B. 227 § 13-61-102(1). 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 (1) control or process the personal data of 100,000 or more consumers annually or (2) 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.

[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). A "covered entity" is a health plan, a health care clearinghouse or a health care provider (like a hospital, nursing home or outpatient clinic) that engages in standard HIPAA transactions, like electronic billing. 45 C.F.R. § 160.103. "Business associate" is defined to include a person

© 2022 Akin Gump Strauss Hauer & Feld LLP

(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. *Id*.

[6] P.A. 22-15 § 3(b)(11)–(14),(16).

[7] *Id*. § 3(b)(15).

[8] *Id*. § 3(c).

[9] *Id*. § 3(b)(1).

[10] *Id*. § 3(b)(8).

[11] *Id*. § 3(b)(10).

[12] *Id*. § 3(b)(2).

[13] *Id*. § 3(b)(3)–(5).

[14] *Id*. § 3(b)(9).

[15] *Id*. § 1(18).

[16] *Id*.

[17] *Id*. § 1(7).

[18] *Id*. § 6(a)(4).

[19] *Id*. § 1(27).

[20] *Id*. § 1(11). "Dark pattern" is defined by this law as " (A) a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and (B) includes, but is not limited to, any practice the Federal Trade Commission refers to as a 'dark pattern.'"

[21] *Id*. § 1(6).

[22] *Id*. § 4(c)(2).

[23] *Id*. § 4(a)(5).

[24] Like in Colorado—and unlike in Virginia—CTDPA data portability rights apply to all consumer personal data, not just such data that was originally provided by the consumer.

[25] *Id*. § 4(a).

[26] *Id*. § 4(b).

[27] *Id*. § 4(c)(1).

[28] *Id*. § (1)(26).

[29] 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"); *see also* Cal. Civ. Code § 1798.140(t) (providing that the term sale means "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration").

[30] P.A. 22-15 § 1(26).

[32] *Id*. § 7(b).

[33] *Id*. § 6(c).

[34] *Id*. § 6(a)(1).

© 2022 Akin Gump Strauss Hauer & Feld LLP

[35] *Id.* § 6(a)(2).

[36] *Id.* § 6(a)(3).

[37] *Id.* § 6(a)(4).

[38] *Id.* § 6(a)(5).

[39] *Id.* § 6(e)(1)(B).

[40] *Id.* § 6(a)(6).

[41] *Id.* § 8(a); the intrusion upon solitude or seclusion, or private affairs must be "offensive to a reasonable person."

[42] *Id.* § 8(b).

[43] *Id.* § 8(c).

[44] *Id.* § 8(f).

[45] *Id.* § 8(e).

[46] *Id.* § 6(a)(7); Cal. Civ. Code § 1798.120(c). The CCPA requires obtaining consent from consumers of at least 13 years of age but less than 16 before processing their personal data.

[47] *Id.* § 6(e)(1)(A)(i).

[48] *Id.* § 6(e)(1)(A)(ii).

[49] *Id.* § 10(e); C.T. Gen. Stat. § 42-110b (2016).

[50] *Id.* § 11(b).

[51] *Id.* § 11(c).

[52] *Id.* § 12(a).

[53] *Id.* § 12(d).

akingump.com

© 2022 Akin Gump Strauss Hauer & Feld LLP