OLR Bill Analysis

sHB 6002

AN ACT SUBJECTING STATE AGENCIES TO THE SAME DATA PROTECTION AND PRIVACY LAWS AS THE PRIVATE SECTOR.

SUMMARY

This bill removes provisions that exempt the state from coverage under the Connecticut Data Privacy Act (CTDPA), specifically its provisions on consumer data privacy and online monitoring; consumer health data privacy; and online services, products, or features and minors. In doing so, it generally subjects the state to these laws' requirements and limitations (it is unclear, however, if this subjects the state to CTDPA's provisions on consumer health data privacy, and online services, products, or features and minors).

Among other things, bringing the state under these laws:

1. gives residents certain rights regarding their state-controlled personal data (e.g., to delete their personal data and opt out of personal data processing for certain purposes);

2. requires the state to (a) limit the collection of personal data to what is adequate, relevant, and reasonably necessary and (b) implement reasonable data security practices; and

3. prohibits the state from processing sensitive data (e.g., data revealing certain traits or status or precise geolocation) without consent.

To the extent it subjects the state to CTDPA's provisions on consumer health data privacy, and online services, products, or features and minors, the bill would also:

1. prohibit the state from giving an employee or contractor access to consumer health data unless they have a contractual or

statutory duty of confidentiality and

2. require the state to use reasonable care to avoid causing any heightened risk of harm to minors through certain online services, products, or features.

(It is unclear how these provisions would be enforced against the state, however, as violations of these laws are a violation of the Connecticut Unfair Trade Practices Act and exclusively enforced by the attorney general, who would also have to defend the state in an enforcement action.)

EFFECTIVE DATE: January 1, 2026

CONSUMER DATA PRIVACY AND ONLINE MONITORING

The bill removes an exemption for the state under the CTDPA's provisions on consumer data privacy and online monitoring. Under current law, these provisions apply to persons that conduct business in the state or that produce products or services targeted to state residents, and that during the preceding calendar year controlled or processed the personal data of at least (1) 100,000 consumers, excluding personal data controlled or processed solely to complete a payment transaction, or (2) 25,000 consumers and derived more than 25% of their gross revenue from selling personal data. The bill also applies these provisions to any state body, authority, board, bureau, commission, district or agency.

By extending CTDPA's provisions on consumer data privacy and online monitoring to cover the state, the bill, among other things:

1. gives state residents rights to (a) confirm whether the state is processing their personal data and access their personal data; (b) correct inaccuracies in their personal data; (c) delete personal data provided by, or obtained about, them; (d) obtain a copy of their personal data processed by the state; and (e) opt out of personal data processing for certain purposes (e.g., targeted advertising, personal data sales);

2. requires the state to (a) limit the collection of personal data to

what is adequate, relevant, and reasonably necessary; (b) not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which it is processed, as disclosed to the resident, without the resident's consent; (c) establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data; (d) not process a resident's sensitive data without consent; (e) have an effective way for a resident to revoke their consent; and (f) not process a resident's personal data for targeted advertising, or sell it without consent;

3. requires the state to give residents a reasonably accessible, clear, and meaningful privacy notice that includes certain information (e.g., the categories of personal data processed by the state, and how they may exercise their rights);

4. requires the state to conduct and document a data protection assessment for each of its processing activities that presents a heightened risk of harm to a resident; and

5. requires the state, if it has de-identified data, to (a) take reasonable measures to ensure that it cannot be associated with an individual; (b) publicly commit to maintaining and using it without attempting to re-identify the data; and (c) contractually obligate any recipients of the data to comply with all provisions of the data privacy and security law.

CONSUMER HEALTH DATA PRIVACY

The bill similarly removes an exemption for the state under the CTDPA's provisions on consumer health data privacy. (However, it does not explicitly subject the state to these provisions and it is unclear whether the state is subject to them as a "person" (i.e. an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust, or other legal entity).) To the extent it extends these provisions to cover the state, the bill generally prohibits the state from:

1. giving an employee or contractor access to consumer health data unless they have a contractual or statutory duty of confidentiality;

2. giving any processor (a person who processes personal data on a controller's behalf) access to consumer health data unless the state and processor comply with the law on the processor's duties;

3. using a geofence (technology that uses location detection) to establish a virtual boundary within 1,750 feet of a mental health facility or reproductive or sexual health facility for identifying, tracking, collecting data from, or sending a notification to a consumer about the consumer's consumer health data; or

4. selling, or offering to sell, consumer health data without the consumer's consent.

ONLINE SERVICES, PRODUCTS, OR FEATURES AND MINORS

The bill similarly removes an exemption for the state under the CTDPA's provisions on online services, products, or features and minors (but does not explicitly subject the state to them). To the extent it extends these provisions to cover the state, the bill generally requires the state to:

1. use reasonable care to avoid causing any heightened risk of harm to minors through any online service, product, or feature for residents that it has actual knowledge, or willfully disregards knowing, are minors;

2. obtain a minor's consent (or a parent's or guardian's) before (a) processing a minor's personal data for certain reasons (e.g., targeted advertising or profiling for certain automated decisions) or (b) using a system design feature to significantly increase, sustain, or extend a minor's use of the online service, product, or feature (excluding certain educational services or applications); and

3. conduct a data protection assessment for these online services, products, or features.

BACKGROUND

Related Bill

sSB 1356, favorably reported by the General Law Committee, among other things, expands who is covered under CTDPA by lowering the applicability threshold and including those who (1) control or process a consumer's sensitive data or (2) offer a consumer's personal data for sale in trade or commerce. It also removes current exemptions to apply it to additional entities.

COMMITTEE ACTION

Government Administration and Elections Committee

Joint Favorable
Yea 19 Nay 0 (03/26/2025)