

Connecticut Senate Bill 2 Two-Pager Cheat Sheet

Created by: **Tatiana Rice**, Deputy Director of U.S. Legislation

Overview: Connecticut SB 2 is a comprehensive and risk-based artificial intelligence (AI) regulation. This overview highlights provisions governing the private sector's use of AI including developer and deployer obligations, consumer rights for transparency and the ability to appeal, and enforcement.¹ If passed, CT SB 2 would become effective February 1, 2026.

<u>Scope of Regulation</u>		<u>Key Terms</u>
<p style="text-align: center;"><u>Regulated Entities</u></p> <p><u>Developers:</u> Any person doing business in the state that develops, or intentionally and substantially modifies an artificial intelligence system, including a general-purpose or high-risk AI system. (Sec. 1(7)).</p> <p><u>Deployers:</u> Any person doing business in the state that deploys a high-risk AI system. (Sec. 1(6)).</p>	<p style="text-align: center;"><u>Regulated Systems</u></p> <p><u>High-Risk AI System:</u> Any artificial intelligence system that when deployed, makes, or is a substantial factor in making, a consequential decision. (Sec. 1(10)).</p> <p><u>General-Purpose AI Model:</u> Any form of artificial intelligence that displays significant generality, is capable of performing a wide range of tasks, and can be integrated into a variety of downstream uses. (Sec.1(8)).</p>	<p><u>Consequential Decision:</u> Any decision that has a material, legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of: (A) Criminal assessment; (B) Education; (C) Employment; (D) Financial or lending services; (E) Essential government services; (F) Healthcare service; or (G) Housing, insurance, or legal services. (Sec. 1(3)).</p> <p><u>Substantial Factor:</u> A factor that assists in making, and is capable of altering the outcome of, a consequential decision, including any content, decision, prediction, or recommendation concerning a consumer that is used as a basis to make a significant decision about the consumer. (Sec. 1(13)).</p>

<u>High-Risk AI Systems</u>		
<u>Developer Obligations</u>	<u>Deployer Obligations</u>	<u>Consumer Rights</u>
<p><u>Duty of Care:</u> Use reasonable care to protect consumers from known or reasonably foreseeable risks of algorithmic discrimination. (Sec. 2(a)).</p> <p><u>Deployer Disclosure:</u> Provide disclosures and documentation to deployers regarding intended use, known or foreseeable risks, a summary of data used to train the system, possible biases, risk mitigation measures, and performance, amongst other items. (Sec. 2(b)).</p> <p><u>Publicly Available Statement:</u> Maintain a publicly available</p>	<p><u>Duty of Care:</u> Use reasonable care to protect consumers from known or reasonably foreseeable risks of algorithmic discrimination. (Sec. 3(a)).</p> <p><u>Risk Management Policy:</u> Maintain a risk management policy that governs high-risk AI use, which specifies processes and personnel used to identify and mitigate algorithmic discrimination. (Sec. 3(b)(1)).</p> <p><u>Impact Assessment:</u> Annually conduct (and upon each intentional and substantial modification) an impact assessment that details the purpose, intended use, risk of algorithmic discrimination, steps to mitigate such risks, description of data used and produced, performance, transparency measures, and post-deployment monitoring. Impact assessments must be retained for at least three years. (Sec. 3(c)(1)-(2), (5)).</p> <p><u>Pre-Deployment Statement of Use:</u> Provide consumers</p>	<p><u>Right to Pre-Use Notice:</u> Must be informed of any high-risk AI system used to make, or be a substantial factor in making, a consequential decision about the consumer, and a statement disclosing the purpose and nature of the system. (Sec. 3(e)(1)(A),(C)).</p> <p><u>Right to Exercise Data Privacy Rights:</u> Must be informed of the right to opt-out of profiling in furtherance of solely automated decisions, under the Connecticut Data Privacy Act, and have the means to exercise those rights, if the deployer is a controller under the CTDPA. (Sec. 3(e)(1)(B)).</p> <p><u>If an adverse consequential decision is</u></p>

¹ Beyond the private-sector regulations, the bill also: creates a new working group to make recommendations regarding generative and general-purpose AI models (Sec. 17), provides partnership between legislators and fellows at the Connecticut Academy of Science and Engineering (Sec. 8), governs deepfakes in political communications (Sec. 9), prohibits the dissemination of synthetic non-consensual intimate images (Sec. 10), creates the Chief Workforce Officer to advise on workforce development policy regarding AI (Sec. 11), requires additional strategy regarding state agency use of generative AI (Secs. 12 and 13), and the creation of a programs, funds, and partnerships to encourage in-state AI talent, innovation, and development (Secs. 14 - 16, 18, 19).



summary of high-risk systems made available to deployers and risk management for algorithmic discrimination. (Sec. 2(d)).

subject to a high-risk system, a statement disclosing information about the high-risk AI system in use, including purpose, nature of the consequential decision, description of how the system assesses information to reach a decision, and sources of personal data processed, among other details. (Sec. 3(e)(1)(C)).

Provide Consumer Rights: Must inform consumers of their rights under the Act and the Connecticut Data Privacy Act and provide the means for the consumer to exercise such rights. Must respond to consumer rights requests within 45 days. (Sec. 3(e)(1)).

Publicly Available Statement: Must make a statement regarding the use of a high-risk AI system available for public inspection. (Sec. 3(f)).

made from the use of a high-risk AI system: (Sec. 3(e)(2))

- **Right to Explanation:** The consumer must be provided a statement explaining the principal reason for the decision, data used in the decision, and the data source.
- **Right to Correct:** The consumer must be provided the opportunity to correct any inaccurate personal data used by the high-risk AI system in the decision.
- **Right to Appeal:** The consumer must be provided an opportunity to appeal that decision for human review, if technically feasible.

Other Requirements

AI Interaction Disclosure: Any person or entity that deploys an artificial intelligence system intended to interact with consumers must disclose to the consumer that they are engaging with an AI system. (Sec. 4)

Watermarking: Developers of artificial intelligence, including general-purpose AI models, must ensure that any synthetic digital content is marked and detectable as such in a manner that is technically feasible and consistent with nationally or internationally recognized standards. (Sec. 5(a)).

Attorney General Disclosures and Enforcement

The Attorney General shall have exclusive authority to enforce. (Sec. 8(a)). The Attorney General may not bring an action for claims otherwise being brought by the Commission on Human Rights and Opportunities for the same conduct. (Sec. 8(f)(3)).

Attorney General Disclosures: Developers and deployers must provide all required documentation to the Attorney General upon request. (Sec. 2(f), (3)(i)).

Right to Cure: Developers and deployers have a 60-day right to cure any alleged violations until June 30, 2026. (Sec. 8(b)).

Safe Harbors and Exceptions

Rebuttable Presumption: Developers and deployers of high-risk AI systems maintain a rebuttable presumption of reasonable care if they are compliant with the relevant bill provisions. (Sec. 2(a), 3(a)). **This does not protect entities from enforcement actions by the Connecticut Commission on Human Rights and Opportunities under existing state and federal anti-discrimination statutes.*

Impact Assessment Interoperability: If a deployer completes an impact assessment to comply with another relevant law or regulation, such impact assessment may be used to satisfy this Act's impact assessment requirements. (Sec. 3(c)(4)).

Small Business Exceptions: If a small business deployer meets certain requirements, they do not need to maintain a risk management program or conduct an impact assessment. They are still subject to a duty of care and must provide the relevant consumer notices and rights. (Sec. 3(g)).

Affirmative Defense: A developer or deployer (1) discovers a violation through internal testing or red-teaming, (2) cured such violation, and (3) otherwise complies with the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework or another nationally or internationally recognized risk management framework. (Sec. 8(f)).



