

# Texas Responsible Artificial Intelligence Governance Act (HB 149) Summary



*In effect as of*  
**January 1,  
2026**

## APPLICABILITY

The law applies to any person who:

- Promotes, advertises, or conducts business in Texas;
- Produces a product or service used by Texas residents; or
- Develops or deploys an artificial intelligence (AI) system in Texas

It covers both developers (those who develop an AI system that is offered, sold, leased, given, or otherwise provided in Texas) and deployers (those who deploy AI systems for use in Texas).

## KEY DEFINITIONS

**Artificial Intelligence System:** Any machine-based system that, for any explicit or implicit objective, infers from inputs the system receives how to generate outputs—such as content, decisions, predictions, or recommendations—that can influence physical or virtual environments.

**Consumer:** A Texas resident acting only in an individual or household context (not in a commercial/employment context).

**Biometric Identifier/Data:** Refers to data generated by automatic measurements of an individual's biological characteristics and includes retina or iris scan, fingerprint, voiceprint, or other unique biological pattern or characteristic that is used to identify a specific individual. This does not include a physical or digital photograph or data generated from a physical or digital photograph, a video or audio recording or data generated from a video or audio recording, or information collected, used, or stored for healthcare treatment, payment, or operations under HIPAA.

**Protected Class:** A group or class of persons with a characteristic, quality, belief, or status protected from discrimination by state or federal civil rights law, and includes:

- Race
- Color
- National Origin
- Sex
- Age
- Religion
- Disability

**Governmental Entity:** Any department, commission, board, office, authority, or other administrative unit of Texas or any political subdivision of the state, that exercises governmental functions under the authority of state law, excluding hospital districts and higher ed institutions.

## DUTIES AND PROHIBITIONS

**Disclosure to Consumers:** Governmental agencies and other persons must clearly and conspicuously disclose to any consumer, before or at the time of interaction, that they are interacting with an AI system. This must be in plain language and may not use dark patterns. For healthcare, disclosure must be provided by the date of first service or as soon as possible in emergencies.

**Manipulation of Human Behavior:** It is prohibited to develop or deploy an AI system in a manner intentionally aiming to incite or encourage physical self-harm, harm to others, or criminal activity.

**Social Scoring:** Governmental entities may not use AI systems to evaluate/classify individuals or groups based on social behavior or personal characteristics to assign social scores that could result in detrimental/unjustified treatment or infringe on legal rights.

**Biometric Data Capture:** Governmental entities cannot use AI to uniquely identify a specific individual using biometric data or the targeted or untargeted gathering of images or other media from the Internet or any other publicly available source without the individual's consent, if the gathering would infringe on any right of the individual under the US Constitution, the Texas constitution, or state or federal law.

**Constitutional Protection:** Prohibits developing or deploying AI systems with the sole intent to infringe, restrict, or impair rights guaranteed under the U.S. Constitution.

**Unlawful Discrimination:** Prohibits developing or deploying AI with the intent to unlawfully discriminate against protected classes. Disparate impact is not sufficient by itself to demonstrate an intent to discriminate. Certain insurance and financial entities are considered compliant if they meet other federal/state regulations.

**Sexually Explicit Content and Child Protection:** Prohibits development/distribution of AI systems with the sole intent of producing, assisting or aiding in producing, or distributing:

- Visual material, deep fake videos or images, or simulated sexual conduct (such as text-based conversations that describe sexual conduct) involving children.

## REGULATORY SANDBOX PROGRAM

- Establishes a regulatory sandbox program under the Texas Department of Information Resources for testing innovative AI systems for up to 36 months without full regulatory authorization. Extensions are possible for good cause.
- Applicants must describe the AI system, its intended use, potential impacts on consumers/privacy/public safety, mitigation plans, and compliance with federal law.
- Participants must submit quarterly performance/risk/feedback reports; the Department submits annual reports to the legislature.
- Sandbox does not waive core Subchapter B requirements (i.e., basic safety/discrimination protections).

## PUBLISHING & NOTICE REQUIREMENTS

- Upon request during civil rights investigations initiated by the state's attorney general in response to a consumer complaint, developers or deployers must provide the following information:
  - A high-level description of the purpose, intended use, deployment context, and associated benefits of the AI system
  - A description of the type of data used to program or train the AI system
  - A high-level description of the categories of data processed as inputs for the AI system
  - A high-level description of the outputs produced by the AI system
  - Any metrics the business uses to evaluate the performance of the AI system
  - Any known limitations of the AI system
  - A high-level description of the post-deployment monitoring and user safeguards the business uses for the AI system, including, if the person is a deployer, the oversight, use, and learning process established by the person to address issues arising from the system's deployment
- Disclosures must be made clearly on websites or via hyperlinks to separate webpages. Disclosures are still required—even if an AI interaction seems obvious to a reasonable consumer.

## ENFORCEMENT

- Exclusive enforcement is by the Texas Attorney General's Office, except for certain agency actions post-adjudication.
- No private right of action under this law.
- The Attorney General maintains an online complaint mechanism. If a complaint is made, civil investigative demands may be issued for information.
- Notice of violation must be given; violators have 60 days to cure and provide documentation before penalties are pursued.
- Civil Penalties:
  - Curable violation: \$10,000–\$12,000 per violation
  - Uncurable violation: \$80,000–\$200,000 per violation
  - Continued violation: \$2,000–\$40,000 per day
  - Agency-imposed sanctions (for licensees): up to \$100,000

While TRAIGA does not include a risk mitigation policy requirement, it provides certain safe harbor provisions to protect against liability under the Act, including:

- If a third party misuses the AI system in violation of the Act, or
- If a violation is discovered through certain enumerated means, such as:
  1. Feedback mechanisms,
  2. Testing (e.g., red teaming),
  3. Following state established guidelines (this may include future guidelines published by the Texas Artificial Intelligence Council), or
  4. An internal review process if the AI system substantially complies with the National Institute of Standards and Technology's (NIST's) AI Risk Management Framework or other nationally or internationally recognized risk management framework. Continued violation: \$2,000–\$40,000 per day

There are no penalties for undeployed AI systems.

## EXEMPTIONS

- Exempts certain biometric uses by financial institutions, AI system use for security/fraud prevention, and data processed for health care operations under HIPAA.
- Insurance entities and federally insured financial institutions are deemed compliant if following relevant federal and state laws and regulations.

## TEXAS AI COUNCIL

Establishes a Texas Artificial Intelligence Council:

- Seven-member public council, appointed by state leadership, to advise the legislature and coordinate with agencies on AI ethics, policy, and innovation.
  - It is created to ensure artificial intelligence systems are ethical and developed in the public's best interest and do not harm public safety or undermine individual freedoms by finding issues and making recommendations to the legislature.
- Functions include issuing reports, training programs, and making recommendations—but the council cannot adopt binding rules or override state agencies.

## REPORTING & STATE AGENCY REQUIREMENTS

- State agencies must evaluate and report on their use of AI systems, including in legislative budget requests and information technology inventories.
- The Department of Information Resources compiles agency AI usage, security, and compliance information.



Stay tuned to the [DCI Consulting Blog](#) and the [DCI website](#) for updates on state, local, and federal AI laws and regulations, and reach out to [sales@dciconsult.com](mailto:sales@dciconsult.com) to find out how DCI can help your organization maintain compliance.