State AI Compliance in Practice

A legal and operational deep dive for governance risk and compliance professionals

GRC Careers Reference Library | Deep Dives
Research checked November 17, 2026

What state AI compliance requires in practice

An organization can buy one AI tool and acquire several different compliance obligations. The questions that determine coverage include who uses the tool, where the affected person is located, what decision the output influences, and whether a human independently evaluates the result. A vendor statement that a product is compliant cannot answer those questions for every deployment.

This report examines selected laws and regulations in fifteen states: California, Colorado, Connecticut, Illinois, Maine, Maryland, Minnesota, Nevada, New York, Oregon, Tennessee, Texas, Utah, Virginia and Washington. New York City is treated separately as a local jurisdiction. The analysis covers employment, consequential decisions, consumer profiling, chatbot safeguards, health data and selected content protections. Each legal finding has a numbered source and a section reference. Implementation recommendations and worked examples are our analysis.

The practical conclusion is to build a record for each use of AI that connects the applicable legal provision to a responsible owner, an operating procedure and evidence that the procedure works. Shared controls can reduce repeated work, while jurisdiction-specific requirements remain visible.

Scope and date. Research checked November 17, 2026. This is a detailed implementation report for the identified regimes, not a fifty-state inventory or a finding that a particular organization complies. It does not exhaust every law within the fifteen states. Frontier-model development, training-data transparency, elections, insurance, medical devices and public-sector procurement require separate inventories. Washington provenance and Tennessee impersonation are included to illustrate distinct content risks. Federal obligations and case-specific court orders require their own review.

Read the legal status before the obligation

A statute is enacted by a legislature. A regulation is adopted by an agency under delegated authority. A proposed rule can explain the direction of a rulemaking, but its proposed duties should not be presented as binding. An agency announcement can verify a date or explain administration; the underlying legal text remains the source for the requirement.

Jurisdiction and regime	Status on the research date	Relevant date
California employment discrimination rules	Adopted regulations in effect [4–6]	October 1, 2025
California CCPA ADMT rules	Adopted; specific ADMT compliance begins later [7–8]	January 1, 2027

Jurisdiction and regime	Status on the research date	Relevant date
California workplace ADS statute	Enacted; operative later [10–12]	July 1, 2027
Colorado ADMT replacement	Enacted replacement; principal requirements apply later [1]	January 1, 2027
Colorado implementing rules	October interim draft reviewed; not treated here as final [2–3]	Verify adoption before relying on draft details
Illinois employment AI statute	In effect; May rule proposal was withdrawn [13,15]	January 1, 2026
Texas HB 149	In effect [16]	January 1, 2026
New York companion protections	Existing Article 47 duties plus forthcoming Article 48 [17–22]	Article 48 starts January 1, 2027
Utah consumer and mental health AI laws	In effect; current compilations include 2026 changes [23–24]	Use current code section numbers
Connecticut profiling provisions	Current review must include 2026 amendments [25]	Relevant amendments July 1, 2026
New York City hiring tools	Local law and adopted rules; enforcement underway [26–28]	Enforcement July 5, 2023
Maryland interview facial recognition	Existing employer consent statute [29]	Current § 3-717
Maryland consumer privacy	Enacted; current duties and algorithm assessments [30–35]	October 1, 2025; act § 2 also addresses prospective processing
Washington companion chatbots	Enacted; operative later [37]	January 1, 2027
Washington content provenance	Enacted; covered-provider threshold [38]	February 1, 2027
Washington consumer health data	Existing targeted privacy regime [39–42]	Principal 2024 commencement dates have passed
Oregon companion chatbots	Enacted, Chapter 85 [43–44]	January 1, 2027
Nevada mental health AI	Enacted; principal restrictions in effect [45–46]	July 1, 2025
Maine chatbot and therapy laws	Current disclosure law plus 2026 therapy restrictions [47–50]	Therapy act July 29, 2026

Jurisdiction and regime	Status on the research date	Relevant date
Minnesota consumer profiling	Rights in effect; initial mandatory cure period expired [51–53,59]	July 31, 2025; cure provision ended January 31, 2026
Virginia consumer profiling	Existing consumer rights and assessment duties [54–56]	Use current code and § 580(G) processing-date rule
Tennessee simulated voice and likeness	Enacted ELVIS Act [57]	July 1, 2024

A future effective date does not establish a general exemption from laws already in force. Keep separate entries for existing duties and forthcoming changes. The Colorado discussion below addresses the enacted 2027 replacement; it should not be used as an assessment of a deployment's obligations during the 2026 transition.

How to determine which requirement governs a deployment

Start with a particular action and follow it through five questions. First, identify the actor: employer, developer, deployer, consumer-data controller, processor or chatbot operator. Second, establish the territorial connection using the provision itself. Third, identify the protected person and context. Fourth, test the regulated function, including actual influence on a decision or the creation of biometric data. Fifth, identify the legal version and date. A positive answer under one law does not substitute for the others.

Recommended evidence. Keep the relevant contract, product configuration, input and output examples, affected locations, entity facts and dated legal conclusion together. Record uncertainty explicitly. For example, the fact that a recruiting supplier operates in Maryland does not alone establish that every customer interview satisfies Maryland's facial-template trigger. Likewise, a privacy law's reference to employment opportunities does not eliminate a separate employment-context exclusion. [29–31,52,60–61]

Separate activities within one product. Listing a vacancy, directing a visitor to an employer, ranking applicants, running a paid career appointment and operating a conversational assistant create different factual records. This report does not assume that an educational publisher performs automated hiring. Adding a ranking feature or conversational memory should trigger a new review because the legal facts have changed.

Colorado requires a decision and evidence analysis

SB 26-189 applies its principal duties to consequential decisions made on or after January 1, 2027. Covered domains include education, employment, housing, finance or lending, insurance, health care and essential government services or benefits. ADMT must materially influence the decision; the definition addresses nontrivial outputs affecting outcomes through ranking, scoring or similar influence. Administrative assistance has specified exclusions. [1, § 1, C.R.S. § 6-1-1701; act § 5]

Developers must provide intended-use, training-category, limitation and use or monitoring documentation, plus material-update notices. Deployers give notice before covered use and adverse-outcome information within thirty days. Correction and reconsideration rights apply, with human reconsideration qualified by commercial reasonableness. Deployer compliance records are retained for at least three years after the decision, or longer under other applicable law. [1, §§ 6-1-1702 through 1705]

The attorney general enforces these duties; the statute creates no new private right of action. Check sector provisions and exceptions separately. [1, §§ 6-1-1706, 1708 and 1709]

Implementation recommendation

Begin with the decision process. Write down what information a person sees, whether a score removes anyone from consideration, and whether reviewers can examine applicants who fall below the cutoff. Preserve the configured version and decision pathway. A tool described as a summary assistant may function differently if its summary contains recommendations that staff routinely follow.

Test reconsideration using a deliberately incorrect input in a test environment. The reviewer should find the source error, evaluate the corrected evidence and record whether the outcome changes. Assign the adverse-outcome notice to a named operational owner and test its delivery. Retain the record needed for the legal purpose without copying unrelated personal material into every compliance file.

The rulemaking distinction

The Attorney General's page links an October 6, 2026 interim draft of 4 CCR 904-6. That document is proposed implementing text. Its format and statements about a future effective date do not themselves prove adoption. Verify the final adopted filing before converting draft-specific procedures into claimed legal requirements. [2–3]

California has separate employment and privacy requirements

Employment discrimination regulations already apply

The Civil Rights Council's definition covers computational processes that make employment decisions or facilitate human decision-making affecting employment benefits. It includes specified exclusions. [4, 2 CCR § 11008.1]

Section 11009(f) prohibits discriminatory automated-decision systems and selection criteria, subject to available defenses. It expressly makes the quality, recency, scope and results of anti-bias testing, and the response to those results, relevant evidence. This is more specific than a generic request for an annual vendor certification. [5, 2 CCR § 11009(f)]

The recordkeeping rule includes selection criteria and automated-decision system data. Covered employment records generally must be preserved for four years from creation or the relevant personnel action, whichever is later. Complaint-related preservation can require longer retention. [6, 2 CCR § 11013(c)–(d)]

Recommended practice. Ask what the test actually evaluated: the same task, population, model version and configuration used in the organization. Record limitations and remediation. Procurement should obtain export rights for the relevant records before the contract ends, because a system that loses its history on termination can undermine the employer's ability to explain a decision.

CCPA automated decisionmaking has a different trigger

First establish whether the organization is a covered business under Civil Code § 1798.140(d), including the applicable thresholds and related-entity provisions. A nonprofit's position under that definition does not resolve its employment-law obligations. [9]

The adopted privacy definition focuses on technology that replaces or substantially replaces human decision-making. Section 7001(e)(1) requires a human reviewer who understands the output, analyzes it with other relevant information and has authority to make or change the decision. Article 11 addresses significant decisions and sets pre-use notice, access and opt-out requirements, with specified exceptions. [7, 11 CCR §§ 7001(e), 7200 and 7220–7222]

The regulation package became effective January 1, 2026, while ADMT compliance begins January 1, 2027. [8] Under § 7155, covered new processing requires a prior risk assessment; qualifying continuing processing begun before the effective date has a December 31, 2027 assessment deadline. Material changes require updates as soon as feasible and within forty-five calendar days. [7, §§ 7150–7157]

Recommended practice. Observe a reviewer handling an actual test file. A person who clicks approve without examining the evidence gives a weak basis for a claim of independent review. Record the review process and authority, then evaluate each legal definition separately. Hiring-related opt-out exceptions require their own analysis; a notice does not establish an exception.

The 2026 workplace statute needs a separate project

SB 947 adds Labor Code Part 5.5.5, operative July 1, 2027. It restricts specified ADS uses and prohibits sole reliance on ADS for discipline or termination. When an employer primarily relies on ADS, § 1522 requires human corroboration and bars use of an output that cannot be corroborated or is found inaccurate, incomplete or misleading. Section 1524 requires a separate written postuse notice at the time the decision is communicated. [10–12, §§ 1522, 1524 and 1526.7]

Check the statute's definitions, exceptions and enforcement provisions, including §§ 1526.3–1526.6. Section 1526.4 preserves applicable CCPA ADMT requirements. A workplace implementation project should therefore track the privacy rules and this statute separately. [10–11]

Recommended practice. Build the corroboration record around evidence a supervisor can evaluate. For example, verify whether a productivity flag reflects poor work, an approved accommodation, a system outage or a data error. Give the reviewer time and authority to decline the proposed action. Keep the employee communication tied to the actual reason for the decision.

Illinois combines broad employment duties with a specific interview law

The Illinois Human Rights Act makes discriminatory effects from AI use in specified employment activities a civil-rights violation and prohibits using ZIP codes as proxies for protected classes. The notice provision refers to an employee. The statute directs the Department of Human Rights to make implementing rules about notice circumstances, timing and means. [13, 775 ILCS 5/2-102(L)]

The official JCAR report records withdrawal of the May 2026 proposed amendments to 56 IAC 2520. That withdrawn proposal must not be used as an adopted specification for notice. The withdrawal does not repeal the enacted statutory language. Check subsequent rulemaking before asserting a current detailed notice format. [15]

Separately, the Artificial Intelligence Video Interview Act covers employers requesting recorded applicant interviews and applying AI analysis for Illinois-based positions. Section 5 requires advance notice, an explanation and consent before the interview. Section 10 restricts sharing. Section 15 requires deletion within thirty days of an applicant's request, with instructions to recipients to delete copies, including electronic backups. [14, 820 ILCS 42/5, /10 and /15]

Recommended practice. Treat video analysis as its own procurement and intake review. A general recruiting notice may omit the explanation and consent needed for this specific workflow. Confirm that the supplier can identify downstream copies and execute deletion instructions. When a file also falls under another retention duty or a legal hold, counsel should resolve the conflict for the particular record rather than letting the system silently choose one rule.

For other employment AI, inventory the inputs as well as the model. A ZIP-code feature can be visible in an ordinary configuration screen, while a proxy may also enter through a derived feature. Have HR and the technical owner review the documented purpose and use of location data. Providing broader applicant transparency can be a voluntary operational choice; label it accurately while detailed notice rules are being checked.

Maryland requires separate interview and consumer privacy reviews

Interview facial templates have a precise statutory trigger

Labor and Employment § 3-717(b) restricts an employer's use of facial recognition to create a facial template during an employment interview. Applicant consent must take the signed-waiver form in subsection (c), with plain-language identification of the applicant, interview date, consent and whether the waiver was read. Subsection (a) defines both facial recognition and the extracted facial template. This is a targeted biometric interview provision, not a consent rule for every video call or every AI hiring tool. [29]

Recommended implementation. Obtain a written supplier answer describing whether interview images are used for recognition or persistent tracking, whether a template is extracted, and which feature creates it. Verify the answer against the enabled configuration. Preserve the required waiver for a covered use, with access limited to the responsible team. A marketing assurance that the tool does not perform emotion analysis does not answer whether it creates an identifying facial template.

MODPA can affect consumer AI and nonprofit services

Commercial Law § 14-4702 covers qualifying Maryland business or targeted-service activity at either 35,000 consumers in the preceding year, excluding payment-only processing, or 10,000 consumers plus more than twenty percent of gross revenue from personal-data sales. Section 14-4701(h) excludes commercial and employment contexts from the consumer definition. Apply that exclusion to the actual relationship; do not automatically classify every purchase of career help as an employer's hiring record. [30–31]

The Attorney General confirms that nonprofits have no general MODPA exemption, subject to the stated specific exceptions. The agency identifies October 1, 2025 commencement. The original act's § 2 separately addresses prospective processing and April 1, 2026; use the act and current codification together rather than describing the two dates as interchangeable. Current codification is Commercial Law subtitle 47, although the historical enacted PDF used subtitle 46. [34–35]

Section 14-4707 requires collection to be reasonably necessary and proportionate to the requested product or service. Sensitive collection, processing and sharing have a stricter necessity test, and sensitive-data sales are prohibited. The section also requires meaningful notices and disclosures for specified profiling. Consent to a broad privacy policy does not replace these substantive restrictions. Section 14-4710 requires documented, regular assessments of heightened-risk processing, including an assessment for each algorithm used in that processing. It identifies risky profiling, sensitive data, sales and targeted advertising as relevant categories. [32–33]

Enforcement. The Attorney General identifies its enforcement authority and potential civil penalties of up to $10,000 per violation, or up to $25,000 for subsequent violations, alongside other remedies. These are potential statutory remedies, not a forecast that every technical defect produces the maximum penalty. [34]

What a completed Maryland review should show

Recommended record. Separate the interview-biometrics determination from the consumer-data assessment. For a covered personalized consumer tool, list each input, why it is needed, which algorithm uses it, possible harmful outcomes, alternatives and safeguards. Link the assessment to testing and the release decision. If data is removed because it is unnecessary, verify that it also disappears from prompts, exports and supplier logs within the applicable retention arrangements.

Illustrative test. A paid career service proposes to infer a customer's health condition from an employment gap to personalize advice. Ask whether the inference is necessary for the requested service and whether the feature can work without it. This is a proposed use requiring review, not a claim that any GRC Careers service performs that inference. Passing a consent checkbox test would not by itself resolve Maryland's necessity restriction. [31–33]

Texas focuses on prohibited conduct and particular disclosures

The Texas Responsible Artificial Intelligence Governance Act took effect January 1, 2026. Its coverage reaches specified business, product and development or deployment connections to Texas. The disclosure provision addresses government consumer interactions and specified health-care uses. It should not be summarized as a universal duty for every private company to label every AI interaction. [16, §§ 551.002 and 552.051]

Section 552.056 prohibits developing or deploying AI with intent to unlawfully discriminate against a protected class; disparate impact alone is insufficient to establish that intent under this section. Other provisions address additional prohibited conduct. Chapter 552 generally gives enforcement to the attorney general, with a specified state-agency role, and supplies no private right of action under the chapter. [16, §§ 552.052–552.057, 552.101 and 552.106]

Recommended practice. Preserve the business purpose, intended use, input and output categories, known limitations and monitoring approach. These materials make a complaint investigation easier to answer. Do not infer from this statute's intent standard that every discriminatory outcome is lawful under other employment or civil-rights laws. Review the particular conduct and each applicable authority.

A Texas comparison should also identify the difference between a legal requirement and a company-wide practice. A company may choose to disclose AI use consistently across its public interfaces even when one statute imposes a narrower duty. Its internal legal register should still identify which rule actually requires each disclosure.

New York separates existing companion duties from new minor protections

Existing duties depend on the companion definition

General Business Law § 1700(4) defines an AI companion by specified features that simulate a sustained human relationship, and includes exclusions. Section 1701 requires a protocol making reasonable efforts to detect and address suicidal ideation or self-harm, including referral to appropriate crisis services. Section 1702 requires a clear nonhuman notification at the beginning of an interaction, subject to its once-per-day qualification, and at least every three hours during continuing interactions. [17–19]

Article 48 changes the analysis on January 1 2027

S9051B, signed October 28, 2026, adds Article 48, effective January 1, 2027. Its covered AI companion definition extends beyond the existing Article 47 companion definition. Section 1800(8) identifies unsafe features, including simulated human emotions, relationship claims and specified harmful outputs. Read the final B text, since earlier versions remain displayed on the same legislative page. [20, §§ 1800 and 1801; act § 3]

The customer-service and research or technical-assistance exceptions in § 1801(2) contain a functional condition: the system must be unable to respond outside the specified purpose. A description in a product policy does not establish that technical boundary. [21]

Section 1804 provides interim age-assurance requirements when the referenced rules are not in effect. Adult self-declaration alone is insufficient under that fallback. Operators must offer multiple methods, including one without government ID or one preserving anonymity as to the operator. Age-assurance information is purpose-limited and subject to immediate deletion after the attempt, with the stated legal-compliance exception. [22, § 1804(1)–(2)]

Recommended practice. Evaluate actual conversation behavior. Test whether a service assistant answers relationship questions, recalls sensitive personal exchanges or presents itself as having human feelings. A product's label does not settle the statutory definitions. Test the exception's scope controls with adversarial prompts and ordinary user questions. Record the version and result without collecting unnecessary identity documents.

This is particularly relevant to career, education and coaching tools. A service can begin as factual assistance and expand through added memory or conversational features. Review such changes before release. The legal question is whether the specific service and conduct meet the applicable definition and exception, rather than whether the company markets itself as a chatbot business.

Utah distinguishes consumer interactions from mental health chatbots

Utah Code § 13-77-103 requires disclosure in consumer transactions when a person clearly asks whether the interaction uses generative AI. High-risk AI interactions in regulated occupations carry proactive disclosure duties, with rules for verbal and written interactions. Section 13-77-104 provides a disclosure safe harbor with its own conditions. Section 13-77-102 says AI involvement is not a defense to violations of consumer-protection statutes administered by the division. [23]

The mental health chatbot chapter has a separate scope test. Section 13-72a-101 considers conversational functionality and representations or reasonable user belief about therapy or management of mental-health conditions. Sections 201–203 regulate information sharing, advertising and disclosures. Disclosure is required before feature access, after seven days of nonuse at the next interaction, and when asked. Section 201 contains specific sharing exceptions and conditions; it is not a blanket permission to send transcripts to any vendor. [24]

Recommended practice. Route product changes that add wellbeing or therapeutic claims through a fresh scope review. Map the actual recipients of conversations, including model providers, analytics services and advertising systems. For each recipient, record the data, purpose and proposed legal basis. Test the disclosure after a simulated period of nonuse, rather than checking only the first-use screen.

Washington combines current privacy duties with enacted 2027 AI laws

The task force is not a private compliance certification

ESSB 5838, Chapter 163 of 2024, § 2 established a task force to study AI and recommend legislation and guidelines. That enactment does not itself turn its recommendations into a universal private-company AI audit regime. A disclosure should identify the binding provision governing an actual practice rather than claim compliance with the task force as if it were a certification standard. [36]

Companion chatbot duties begin January 1, 2027

ESHB 2225, Chapter 168 of 2026, defines companions by adaptive human-like interaction and the ability to sustain relationships. Section 2 contains operational and other exceptions with conditions. Sections 3–5 require AI disclosure at the start and at least every three hours, hourly notices for covered minors, restrictions on manipulative and sexual content for minors, and a self-harm response protocol with public reporting. The minor-specific trigger is operator knowledge that the user is under eighteen or a chatbot directed to minors. Section 6 applies the Consumer Protection Act. The effective date is January 1, 2027. [37, §§ 2–6 and 9]

Recommended review. Test the features that sustain relationships: memory across sessions, unsolicited emotional prompts, claims of feelings and attempts to prolong engagement. Check the actual behavior of an assistant described as customer service. A disclaimer in the footer cannot establish that the product qualifies for a functional exception. Document the operator's control over the embedded tool as well as the supplier's responsibilities.

Provenance obligations have a different actor and date

E2SHB 1170, Chapter 167 of 2026, becomes effective February 1, 2027. Its covered-provider definition concerns producers of publicly accessible generative systems with over one million monthly users, accessible to Washington consumers for personal use. The statutory generative-media definition concerns images, audio and video. Section 2 requires provenance data and tamper-resistance using commercially and technically reasonable methods. Section 3 excludes business-to-business uses, sales, licensing and distribution; § 4 reserves its Consumer Protection Act enforcement to the Attorney General. Section 6 separately addresses government AI interaction notices. Publishing an AI-assisted article or buying a third-party tool does not alone establish covered-provider status. [38]

Recommended review. Record who produces the system, the relevant user count, distribution model, output media and any exclusion. For a covered media product, preserve output samples and the result of metadata checks after ordinary export and conversion. Explain any technical limitations. Treat the legal reasonableness qualification as an issue requiring evidence, not an automatic exception.

Inferred health data creates a separate privacy question

My Health My Data, RCW 19.373, is already an operative regime. Section .010 includes specified inferred health information derived from nonhealth inputs, including through algorithms or machine learning. Its consumer definition excludes employment contexts. A consumer service and an employer's employee record therefore need separate scope analyses. Section .020 requires a consumer-health privacy policy and prominent homepage link. Section .030 sets separate collection and sharing conditions, including the requested-service necessity provisions. Section .090 applies the Consumer Protection Act. [39–42]

Recommended record. Identify whether the service actually receives or infers covered health data, the relevant relationship, each recipient and the proposed legal condition for collection or sharing. Do not assume all wellbeing-related text is exempt because the supplier is outside HIPAA. Conversely, do not add a health-data collection claim to a policy merely because such data could hypothetically appear. Align the notice with verified operations and review the remaining chapter, including rights, processors and sale authorization, for a covered deployment.

Privacy laws can impose AI related duties without an AI act

Connecticut illustrates the need to review privacy statutes alongside dedicated AI legislation. The 2026 supplement contains profiling-related consumer rights in § 42-518 and assessment requirements in § 42-522. The July 1, 2026 amendments must be distinguished from earlier text printed on the same page. The provisions address significant automated decisions and specified risks, with statutory qualifications. Coverage, exemptions and the consumer definition require separate review under §§ 42-515–42-517. [25]

Recommended practice. Include privacy counsel in the initial scope review. Identify whether the affected person is acting as a consumer, applicant, employee or another kind of individual under the particular statute. A report that lists only laws with AI in their titles can miss relevant rights and assessment duties. Conversely, applying every consumer right to every employee record can produce an inaccurate compliance specification.

Minnesota creates a substantive route to question profiling

Minnesota's Consumer Data Privacy Act became effective July 31, 2025. Section 325M.12 generally uses thresholds of 100,000 consumers, excluding payment-only data, or 25,000 consumers and over twenty-five percent of gross revenue from sales. Its exclusions require an activity- and record-specific review. The consumer definition in § 325M.11(g) excludes commercial and employment contexts, while the significant-decision definition includes employment opportunities. Read both rather than treating the latter as blanket coverage of all applicant records. [52–53,60]

For covered profiling, § 325M.14, subd. 1(f)–(g), provides an opt-out right and a right to question results and receive reasons. Where feasible, the consumer can obtain information about actions that might have secured, or could secure, a different decision. The consumer may review the data used; an inaccurate-data decision carries correction and reevaluation rights. These rights require more than disclosing that an algorithm exists. Subdivision 4 generally sets a forty-five-day response period, subject to its specified conditions. [51]

Recommended implementation. A response owner should be able to retrieve the input snapshot, decision reason, relevant policy and correction route. Test a materially wrong input and verify that the correction reaches the decision process, rather than changing only the account profile. Ask the supplier how it will support an intelligible reason when a model produces a score without an explanation. This operational design is our recommendation for satisfying the rights actually applicable to the service.

Enforcement changes the implementation timeline. Section 325M.20 provides Attorney General enforcement and penalties of up to $7,500 per violation, and creates no private action under that act. The initial thirty-day warning provision expired January 31, 2026. A November 2026 plan should not promise a statutory warning period that has already ended. [59]

Virginia shows why a privacy assessment is different from a bias audit

Virginia Code § 59.1-576 generally requires 100,000 consumers or 25,000 consumers and over fifty percent of gross revenue from sales, alongside the territorial test. Nonprofits are expressly excluded under the statute's

definition and coverage provisions, as are specified other entities and data. Employment-context limits require separate review. This differs materially from Maryland's nonprofit position and thresholds. [54,61]

For covered consumers, § 59.1-577(A)(5) provides an opt-out right for profiling that furthers legally or similarly significant decisions. Sections 577(B)–(C) govern response and appeal procedures. Section 580 requires documented assessments for specified risky profiling and other processing. The assessment weighs benefits against risks and mitigations and must consider context and reasonable expectations. Its processing-date rule and conditions for reusing a comparable assessment matter. A vendor bias audit may supply evidence but does not replace this broader analysis. [55–56]

Recommended implementation. Identify a specific decision, the harm it could cause, the supporting evaluation, the necessity of the data and the safeguards that reduce the risk. Make the approval depend on unresolved issues being closed or explicitly accepted by an authorized owner. A document headed impact assessment is not sufficient when it contains no finding about the deployed configuration.

Section 59.1-584 provides exclusive Attorney General enforcement, a thirty-day notice-and-cure procedure with written assurances, and potential injunctions and civil penalties up to $7,500 for each violation when its conditions are met. This differs from Minnesota's expired initial warning provision. Do not apply one state's cure process to another. [58]

Oregon adds a companion regime with private remedies

SB 1546, enacted as Chapter 85 of 2026, takes effect January 1, 2027. Its companion definition concerns sustained simulated relationships and contains specified exceptions. Section 1 addresses misleading human presentation, evidence-based self-harm detection and response protocols, safeguards for minors, periodic reminders and public annual reporting without identifying users. Section 2 allows an injured individual to seek the greater of actual damages or $1,000 statutory damages for each violation, an injunction and potentially fees. [43–44]

Recommended implementation. Keep the Oregon definition and exception analysis distinct from Washington and New York. Create a test library that exercises the same prohibited behavior across each applicable legal standard, then record the different legal conclusions. Track the source and date of each reporting obligation. A general company promise to keep users safe does not document the protocol, operating tests or required public reporting.

Illustrative boundary. A narrow information service later adds persistent memory and initiates conversations about a user's emotional life. Before release, compare the new behavior with the companion definition and relevant exceptions. Verify the actual limits on conversation rather than assuming the original customer-support purpose still describes the expanded feature. A changed use can require new controls even when the underlying model is unchanged.

Nevada restricts AI mental health services beyond disclosure

AB 406, Chapter 283 of 2025, principally effective July 1, 2025, prohibits specified representations that an AI system provides professional mental or behavioral health care and prohibits making available a system specifically programmed to deliver a service that would constitute that professional practice if performed by a person. Section 7 includes self-help and administrative-support qualifications, investigation authority and penalties up to $15,000 per violation. This is not a regime satisfied simply by telling the user that the therapist is AI. [45]

NRS 629.610 separately restricts providers' direct patient-care use while allowing specified administrative support, subject to privacy and security requirements. The distinction between delivering a professional service and assisting with administration is operationally important. An appointment scheduler and an assistant directing therapeutic treatment cannot be treated as the same approved use merely because they share a vendor. [46]

Recommended implementation. Review marketing, prompts, actual outputs and professional workflows together. Remove unsupported therapeutic claims and prohibit the restricted functionality where the law applies. Test whether the assistant gives individualized treatment directions despite narrower product copy. Retain the configured restrictions and evaluation evidence. A disclosure may remain useful for transparency, but it does not authorize conduct the statute prohibits.

Maine combines commercial chatbot notice with professional boundaries

Current 10 M.R.S. § 1500-DD, reallocated from former § 1500-Y, requires clear disclosure when using a chatbot or other technology in trade or commerce in a way that may mislead a reasonable consumer into believing the interaction is with a person. Violations fall under the Maine Unfair Trade Practices Act. This does not depend on the tool qualifying as a relationship-oriented companion. [47]

Separately, § 1500-EE restricts public provision, advertising or offering of therapy or psychotherapy, including internet-based AI services, unless supplied by a licensed professional, with the stated research exception. LD 2082's parallel professional provisions distinguish administrative and supplementary support and prohibit independent therapeutic decisions, direct therapeutic interaction and unreviewed treatment plans. Supplementary support requires the specified written disclosure and consent. The chapter was signed April 13, 2026; the session's general nonemergency commencement was July 29, 2026. [48–50]

Recommended implementation. Test a consumer transaction in the ordinary customer journey: chat opening, product recommendation, payment handoff and escalation to staff. The notice should be visible at the point where the user could be misled. Separately classify any feature that moves toward therapy. Career coaching, factual educational assistance and professional therapy should be described and operated according to their actual functions, rather than relying on one general AI disclaimer.

Tennessee protects real and simulated voice and likeness

The ELVIS Act, Public Chapter 588 of 2024, effective July 1, 2024, adds identifiable simulated voice to Tennessee's personal-rights protections. Section 6 addresses specified unauthorized advertising and fundraising uses, knowing public distribution of an unauthorized voice or likeness, and specified technologies primarily producing an identifiable individual's image, voice or likeness. Section 10 contains First Amendment-related qualifications. These are personal-rights and civil-liability questions, distinct from data-protection assessments or chatbot disclosures. [57]

Recommended implementation. Before producing an AI spokesperson, endorsement or fundraising appeal, identify the person whose voice or likeness is used, the intended use, permission and any relevant exception. Keep the authorization with the asset and its distribution limits. A generic license from an AI vendor does not itself establish the individual's authorization. A label saying that content was generated by AI does not answer whether the voice or likeness was authorized.

New York City adds a distinct hiring tool regime

New York City's rule is local. Administrative Code § 20-871 requires a bias audit no more than one year before use of a covered AEDT and public availability of the required audit summary. It also specifies notices to covered candidates or employees residing in the city at least ten business days before use. [26]

The adopted rules define substantial assistance by reference to sole reliance, greater weighting than any other criterion, or overriding other conclusions. Sections 5-301 and 5-302 specify audit and data requirements. Section 5-303 addresses publication, including keeping the summary posted for at least six months after the latest use. Section 5-304 explains notices and makes clear that the rules do not themselves require an alternative selection process. Other accommodation duties require separate review. [27, 6 RCNY §§ 5-300–5-304]

Recommended practice. Ask for the audit's date, tool identification, data sources, auditor independence and applicable results. Check that the published summary matches the tool under review. Calendar renewal and website checks. If a vendor changes the model or the employer changes its use, reassess whether the existing audit remains relevant rather than treating the original report as permanent approval.

A worked example of a national hiring platform

Illustrative facts. A service organization uses a vendor to rank applicants. Staff usually invite only the top ten for interviews. Recruiters see the ranking before reading applications. The platform also offers AI analysis of recorded interviews. Positions are based in several states and New York City. Assume the relevant entity and territorial coverage tests have been met; those tests must be documented separately in a real assessment.

Review question	Analysis and action
Does a person make the final choice?	That fact alone does not settle the different influence and automation tests. Observe which applicants the person actually considers and what authority the person exercises. [1,4,7,27]
Is the vendor audit enough?	Check its match to the tool and use, its age, data and required public summary for the NYC workflow. Evaluate the evidence relevant to California discrimination claims separately. [5,26–27]
May video scoring start immediately?	For the covered Illinois video workflow, complete the explanation, notice and consent process before the interview. Verify the sharing and deletion process. [14]
Does video analysis create a facial template?	For a covered Maryland interview use, verify the enabled function and obtain the statutory signed waiver before proceeding. Ordinary video and identifying-template extraction are different facts. [29]
What belongs in the 2027 project?	Assess Colorado's enacted replacement and California's ADMT requirements separately. Build the relevant notices, rights procedures and records around the actual use. [1,7–8]

The recommended review record

Record the hiring purpose and the approved workflow, then attach evidence for each conclusion: the configured model version, a sample ranking, the human review instructions, the applicable audit, notice delivery and a test

correction request. Document an unresolved issue as unresolved, with an owner and due date. Do not convert an unanswered supplier question into an assumption of compliance.

A meaningful completion test is to reconstruct one simulated rejection. A reviewer should be able to identify the relevant input, the tool output, the person's independent analysis, the notice that would be sent and the route for raising an error. If the organization cannot reconstruct that path, the records and procedures need more work before approval.

A worked example of a nonprofit service assistant

Illustrative facts. A nonprofit introduces a conversational assistant to explain programs. A later update adds remembered personal concerns and supportive dialogue. Another team wants the assistant to recommend which applicants should receive a scarce service. These are separate uses even if they share a model.

Recommended analysis. Review the informational assistant, any relationship-like conversational behavior and service-eligibility recommendations as separate inventory entries. For New York, compare actual functionality with the existing and forthcoming companion definitions and the narrow-purpose exceptions. For Utah, evaluate whether the service makes mental-health representations or creates a reasonable belief that it can provide the covered help. For Colorado, test the proposed eligibility use against the covered-domain and material-influence definitions. Do not assume that all nonprofit program allocation is an essential government service. [1,17,20–24]

Recommended completion test. Give the informational assistant questions outside its permitted topic and check whether it actually refuses them. Give the eligibility workflow a deliberately incomplete case and see whether a qualified person can identify the missing information and reconsider the result. Preserve deidentified test evidence. Review the changed use before the product team enables it for the public.

Cross-state analysis: why one notice and one audit are insufficient

The legal trigger determines the control

A notice, consent record, evaluation, assessment and rights procedure answer different questions. Notice tells a person about a use. Consent records a legally relevant choice where required. Evaluation measures a system against a defined task. An assessment weighs an activity's benefits and risks. A rights procedure changes what a person can do after a decision. An organization may need several of these for one deployment; completing one does not prove completion of the others.

Compare the interview examples. Illinois's video law addresses AI analysis of covered recorded interviews. Maryland's provision asks whether facial recognition creates an interview facial template. NYC's hiring regime uses its own AEDT and substantial-assistance definitions. A procurement questionnaire must therefore ask separate factual questions about recording, analysis, identification and decision influence. A single question asking whether the product uses AI loses the information needed to apply the laws. [14,26–29]

Human involvement must be evaluated against the particular law

Recommended test. Observe a reviewer handling an output that is confidently wrong. Determine whether the person notices the error, has access to the underlying evidence, can change the decision and has enough time to do so. Then apply the relevant definition. Do not call a process independent review solely because an employee clicks a confirmation button. Equally, do not assume every assisted decision meets every state's automation test. The cited California, Colorado and NYC provisions deliberately use different concepts. [1,4,7,27]

Exemptions belong to a provision and a context

Maryland and Virginia illustrate why nonprofit status cannot support a nationwide exemption statement. A service can be outside one privacy statute because of an entity exemption and still require a separate analysis under employment, biometric or consumer-protection law. Likewise, employment-context exclusions do not answer the treatment of a separately purchased consumer service. Retain the rationale for each conclusion and trigger reassessment when the entity, data, customer relationship or service changes. [29–34,54,61]

The remedy and enforcement route affect response planning

Recommended response design. Record the regulator or claimant, available remedies, cure qualifications, reporting duties and evidence-preservation needs in the legal register. Oregon expressly creates a private remedy for its companion regime. Minnesota's privacy act creates no private action under that act and its initial warning provision has expired. Virginia retains a specific statutory cure procedure. Washington's provenance act expressly reserves the cited enforcement route to its Attorney General. These differences should appear in the incident playbook, not only in a footnote. [38,43,58–59]

A supplier can support compliance without certifying every deployment

Recommended contract review. Ask for documentation of the enabled features, model and configuration changes, evaluation limits, intended use, downstream recipients, deletion assistance and exportable decision evidence. Assign responsibility for notices, consent, consumer requests and incidents. Test the promised assistance before launch using a simulated request. Record what the customer must do and what the supplier can actually provide. A contractual allocation of tasks should not be mistaken for a legal conclusion that the customer has no remaining duties.

The compliance record should connect law to evidence

The following is a recommended operating design. The rows are not a claim that every cited law independently mandates every listed artifact. Each organization should map the appropriate row to its applicable legal provisions and document exceptions.

Record	Responsible owner	Evidence of completion
Scope decision	Legal with product or HR	Dated facts, cited provision, applicability conclusion, exceptions and next review trigger.
System and use inventory	Product or system owner	Purpose, affected population, jurisdictions, vendor and configured version.
Evaluation	Risk and technical owner	Task-specific results, limitations, remediation and retest outcome.
Notice and consent	HR or service operations	Approved wording, placement, timing and delivery or consent records where required.
Rights and human review	Operations with legal	Working intake, assigned reviewer, authority, response tracking and test case.
Supplier evidence	Procurement	Documentation access, change notices, exports, downstream recipients and deletion assistance.

Record	Responsible owner	Evidence of completion
Retention and deletion	Privacy and records owner	Record-specific schedule, applicable holds, access controls and completed deletion evidence.
Change review	Product governance	Impact of a new model, feature, use, population or legal development and the decision to retest.

Questions to put into a supplier review

- Which specific model and configuration does your documentation cover, and what changes require a new evaluation?
- What information can we obtain to explain a decision, investigate an error and respond to a lawful request?
- How will we receive material change notices, including changes to upstream models or subprocessors?
- Can we export the relevant records when the contract ends, and can you execute deletion instructions across downstream copies?
- What claims do you make about independence, bias testing or legal compliance, and what evidence supports each claim for our intended use?

These are proposed procurement questions. Their legal basis and contractual wording should be adapted to the organization and use. An unavailable artifact should lead to a documented decision about the resulting gap, including whether the use should be restricted or delayed.

Implementation through January 1 2027

For an organization within the relevant 2027 regimes, the following is a proposed work schedule. Existing duties should be addressed immediately; the calendar does not defer them.

Period	Work	Completion evidence
November 18–25	Inventory uses; verify legal coverage and dates; identify owners.	Every consequential or public-facing use has an owner and an applicability record.
November 26–December 9	Obtain supplier records; implement notices and rights processes; evaluate gaps.	A reviewer can trace each applicable requirement to a procedure and evidence.
December 10–23	Run correction, reconsideration, disclosure, deletion and change tests as relevant.	Failures have been corrected or assigned a documented restriction on use.
December 24–31	Recheck legal developments; approve the permitted uses and escalation arrangements.	Named owners approve the documented scope and know when to stop or reassess use.

A practical exercise for AI governance professionals

Choose a fictional hiring or service workflow and prepare a two-page applicability analysis supported by the legal text. Add a control map, a supplier evidence request and one completed test case. Keep personal information out of the portfolio. State which parts are legal findings, which are assumptions and which are recommendations.

Interview question. A supplier says its tool is compliant because a human approves the result and the vendor completed a bias audit. What would you ask before recommending deployment? A strong answer identifies the relevant jurisdiction and use, tests the actual human role, checks the scope and age of the evidence, and maps unresolved issues to an owner. It does not substitute a certification name for a legal analysis.

Source register and publication maintenance

The numbered references below identify the legal text used for each finding. Agency explanations and rulemaking-status records are labeled separately. Short quoted terms in this report are drawn from the cited provisions; the explanatory prose is paraphrased. The California SB 947 entry discloses use of reproduced chaptered text where the official portal blocked retrieval.

Publication maintenance. Keep the research date visible and record substantive revisions. Recheck the Colorado final rule filing, Illinois implementing-rule status, the cited effective dates and any applicable court orders when updating this report. A source that contains earlier and later versions must be read using the version governing the date of the activity. Publish legal changes as corrections to the affected finding and control, with a new review date. For this revision, Maryland and Washington were added and six further state sections were researched: Maine, Minnesota, Nevada, Oregon, Tennessee and Virginia. The report now identifies fifteen states plus NYC. Maintain a separate all-state discovery inventory before describing any publication as a fifty-state survey. An omitted jurisdiction is unassessed here, not a finding that it has no AI-related requirements. Recheck the January and February 2027 Washington dates and Oregon commencement alongside the other scheduled changes.

[1] Colorado enacted ADMT replacement

SB 26-189 signed act, section 1, C.R.S. §§ 6-1-1701 through 1709; section 5. Main duties apply January 1, 2027. Read source text

[2] Colorado proposed implementing rules

Department of Law, October 6, 2026 interim draft, 4 CCR 904-6. Proposed text, not cited as an adopted rule. Read source text

[3] Colorado rulemaking status

Attorney General rulemaking page. Administrative status source, not the statute. Read source text

[4] California employment system definition

2 CCR § 11008.1, Barclays Official California Code of Regulations. Adopted legal text. Read source text

[5] California employment discrimination rule

2 CCR § 11009(f), Barclays Official California Code of Regulations. Adopted legal text. Read source text

[6] California employment records rule

2 CCR § 11013(c) and (d), Barclays Official California Code of Regulations. Adopted legal text. Read source text

[7] California adopted privacy regulations

CPPA approved regulations, 11 CCR § 7001(e), §§ 7150 through 7157, § 7200 and §§ 7220 through 7222. Approved text, September 22, 2025. Read source text

[8] California privacy compliance dates

CPPA announcement, September 23, 2025. Agency explanation of effective and compliance dates. Read source text

[9] California privacy statute coverage

Civil Code § 1798.140(d), in CPPA statutory compilation, January 2025 edition. Used for the business definition, not later monetary adjustments. Read source text

[10] California workplace ADS statute

SB 947, Chapter 859, Statutes of 2026; Labor Code §§ 1520, 1522, 1524 and 1526 through 1526.7. Official legislative record. Read source text

[11] California workplace ADS chaptered text reproduction

Reproduction of enacted SB 947, Chapter 859. Used to read final sections because the official bill portal blocked retrieval. Read source text

[12] California workplace ADS enactment confirmation

Senator McNerney signing announcement, September 30, 2026. Primary status confirmation; not used instead of statutory text. Read source text

[13] Illinois employment AI statute

775 ILCS 5/2-102(L), as amended by Public Act 103-0804, effective January 1, 2026. Read the version applicable to the date at issue. Read source text

[14] Illinois video interview statute

820 ILCS 42, especially §§ 5, 10 and 15. Actual statutory text. Read source text

[15] Illinois proposed rules withdrawal

JCAR Flinn Report, June 26, 2026, DHR Rule Withdrawal, 56 IAC 2520, proposal published at 50 Ill. Reg. 6794. Official legislative rulemaking record. Read source text

[16] Texas enacted AI statute

HB 149 enrolled text, section 4, Business and Commerce Code Chapters 551 and 552, especially §§ 551.002, 552.051, 552.056 and 552.101 through 552.106. Effective January 1, 2026. Read source text

[17] New York existing companion definition

General Business Law § 1700(4), actual codified text. Read source text

[18] New York existing companion safety duty

General Business Law § 1701, actual codified text. Read source text

[19] New York existing companion notification duty

General Business Law § 1702, actual codified text. Read source text

[20] New York enacted minor protections

S9051B, signed October 28, 2026, Chapter 368. Final B text adds General Business Law §§ 1800 through 1805; act § 3 sets January 1, 2027 effective date. Read source text

[21] New York forthcoming scope and exceptions

General Business Law § 1801, actual codified text marked effective January 1, 2027. Read source text

[22] New York forthcoming age assurance

General Business Law § 1804, actual codified text marked effective January 1, 2027. Read source text

[23] Utah general consumer AI statute

Utah Code §§ 13-77-101 through 13-77-106, especially §§ 102 through 104. Official code compilation reflects 2026 renumbering. Read source text

[24] Utah mental health chatbot statute

Utah Code Chapter 13-72a, especially §§ 101 and 201 through 204. Official code compilation includes 2026 amendments. Read source text

[25] Connecticut privacy and profiling statute

Connecticut General Statutes, 2026 supplement, §§ 42-515 through 42-522; use amendments operative July 1, 2026. Read source text

[26] New York City hiring tool law

NYC Administrative Code §§ 20-870 and 20-871; linked code page contains § 20-871. Local law, not a statewide requirement. Read source text

[27] New York City adopted hiring tool regulations

6 RCNY §§ 5-300 through 5-304, April 2023 notice of adoption. Actual adopted text, PDF pages 3 through 10. Read source text

[28] New York City enforcement status

DCWP AEDT page. Agency implementation information; enforcement began July 5, 2023. Read source text

[29] Maryland interview facial recognition

Labor and Employment § 3-717(a)–(c). Actual current statute. Read source text

[30] Maryland privacy coverage thresholds

Commercial Law § 14-4702. Actual current statute; excludes payment-only data from the first threshold. Read source text

[31] Maryland privacy definitions

Commercial Law § 14-4701, especially consumer, consent, sensitive data and profiling definitions. Actual current statute. Read source text

[32] Maryland controller duties

Commercial Law § 14-4707(a), (b), (d) and (e). Actual current statute. Read source text

[33] Maryland algorithm assessments

Commercial Law § 14-4710(a)–(d). Actual current statute. Read source text

[34] Maryland regulator implementation explanation

Attorney General MODPA FAQ. Agency explanation of commencement, nonprofit coverage, enforcement and penalties; not substituted for the statutory duties above. Read source text

[35] Maryland original enacted privacy act

Chapter 455, Laws of 2024, SB 541, especially act §§ 2 and 4. Historical enactment used for commencement and prospective application; current code uses subtitle 47 rather than the original subtitle 46. Read source text

[36] Washington AI task force enactment

ESSB 5838, Chapter 163, Laws of 2024, § 2. Actual session law establishes a task force and recommendations process. Read source text

[37] Washington companion chatbot enactment

ESHB 2225, Chapter 168, Laws of 2026, §§ 2–6 and 9. Actual session law; effective January 1, 2027. Read source text

[38] Washington content provenance enactment

E2SHB 1170, Chapter 167, Laws of 2026, §§ 1–4, 6 and 9. Actual session law; effective February 1, 2027. Read source text

[39] Washington consumer health data definitions

RCW 19.373.010, especially (7), (8) and (23). Actual current statute. Read source text

[40] Washington consumer health privacy notice

RCW 19.373.020. Actual current statute, including homepage publication and new-purpose controls. Read source text

[41] Washington consumer health collection and sharing

RCW 19.373.030. Actual current statute; collection and sharing have distinct conditions. Read source text

[42] Washington consumer health enforcement

RCW 19.373.090. Actual current statute applies the Consumer Protection Act. Read source text

[43] Oregon companion chatbot legal text

SB 1546 enrolled text, §§ 1–2; enacted as Chapter 85, Laws of 2026. Final legislative text read here because the chaptered PDF blocked retrieval. Read source text

[44] Oregon companion chatbot enactment and date

Official joint measure status, SB 1546 entry: Chapter 85 and January 1, 2027 effective date. Administrative enactment record. Read source text

[45] Nevada mental and behavioral health AI enactment

AB 406, Chapter 283, Statutes of Nevada 2025, §§ 7–10, printed pages 1894–1897. Actual session law; principal requirements July 1, 2025. Read source text

[46] Nevada professional use restrictions

NRS 629.610. Actual codified law; administrative support exception and privacy obligations. Read source text

[47] Maine commercial chatbot disclosure

10 M.R.S. § 1500-DD. Actual current statute, reallocated from former § 1500-Y. Read source text

[48] Maine therapy service restriction

10 M.R.S. § 1500-EE. Actual current statute; distinguish the January 2027 licensing-reference change from the existing substantive restriction. Read source text

[49] Maine professional AI support enactment

LD 2082, P.L. 2025, Chapter 687, enacted April 13, 2026, especially § 2 adding 32 M.R.S. § 2113. Actual chapter text; parallel provisions govern other listed licensees. Read source text

[50] Maine commencement calendar

Legislature official session information identifies July 29, 2026 as the general effective date for nonemergency laws of the Second Regular Session. Read source text

[51] Minnesota profiling and reconsideration rights

Minn. Stat. § 325M.14, subd. 1(f)–(h) and subd. 4. Actual current statute. Read source text

[52] Minnesota privacy coverage

Minn. Stat. § 325M.12, subds. 1–2. Actual current statute; thresholds and record- or activity-specific exclusions. Read source text

[53] Minnesota privacy commencement

Attorney General announcement of July 31, 2025 commencement. Agency explanation; substantive duties are sourced to the statute. Read source text

[54] Virginia privacy coverage

Va. Code § 59.1-576. Actual current statute; entity and data exemptions must be assessed separately. Read source text

[55] Virginia profiling rights

Va. Code § 59.1-577(A)(5), (B) and (C). Actual current statute. Read source text

[56] Virginia data protection assessments

Va. Code § 59.1-580. Actual current statute, including processing-date and reuse qualifications. Read source text

[57] Tennessee voice and likeness enactment

Public Chapter 588, Laws of 2024, §§ 3–6, 10 and 13; amends Tenn. Code §§ 47-25-1102, 1103, 1105 and 1107. Actual signed act, downloaded and read directly from the Secretary of State because web retrieval blocked the PDF. Effective July 1, 2024. Read source text

[58] Virginia privacy enforcement

Va. Code § 59.1-584. Actual current statute; attorney general enforcement, cure procedure and civil penalties. Read source text

[59] Minnesota privacy enforcement

Minn. Stat. § 325M.20. Actual current statute; mandatory warning provision expired January 31, 2026. Read source text

[60] Minnesota consumer and profiling definitions

Minn. Stat. § 325M.11(g), (i) and (s). Actual current statute. Read source text

[61] Virginia consumer and profiling definitions

Va. Code § 59.1-575. Actual current statute. Read source text