# Court protective orders and the use of AI in eDiscovery

## Our position

The court's order governs how a firm may use LegalPrizm with protected discovery. Before a firm submits that material, counsel should compare the operative order and any amendments with the configuration and written terms for the service the firm will actually use. This statement describes LegalPrizm's service. It is not legal advice.

## What "local" means in this statement

A local model, or local OCR, is software that runs inside the LegalPrizm deployment, alongside the application. Evidence and queries handled by a local model are not sent to an outside model service. Local does not mean that the software runs in the firm's own office, unless the firm's written deployment terms say so.

## How the reviewed workflow handles evidence

On November 28, 2026, LegalPrizm reviewed a running local search deployment of its software. LegalPrizm carried out the review itself. It was not an independent audit. The review found no step in intake, optical character recognition, indexing or search that submitted case files, excerpts or queries to a generative model. The system stores original files, extracts text and uses local OCR for scanned pages. For semantic search, a local model converts passages and queries into numerical vectors. A second local model locates answer spans in the evidence. The application verifies the selected text against its source and displays cited passages.

This finding applies to that configuration. It does not establish the behavior of a deployment that is configured differently, of an integration with another product, or of tools a firm adopts through LegalPrizm's AI workflow consulting, which is a separate service.

Hosted OCR through Amazon Textract and generative models through Amazon Bedrock are optional services. The reviewed workflow uses neither. LegalPrizm processes evidence only for the services a firm authorizes. Before either service is used on a matter, the firm and LegalPrizm identify the service, the data sent, the model, the region and the retention terms, and counsel obtains any approval the order requires.

## Documents in other languages

Firms receive documents in many languages, and LegalPrizm intends to scan, digitize and analyze them. Today the two models in the reviewed workflow differ. BGE-M3, which ranks passages for semantic search, is a multilingual model. TinyRoBERTa, which selects answer spans, is an English-language model, so its selections should be relied on for English text only. Before using LegalPrizm on documents in another language, confirm with LegalPrizm which languages the OCR and each model support for that matter.

## Applying an order to a matter

Orders differ on whose data is protected, which tools and recipients are permitted, and whether counsel must give notice, obtain written consent or seek court approval. Some reach machine learning broadly enough to include embedding or extractive models. A firm should use a feature with protected material only when the order permits it and any required steps are complete.

## Who can access a firm's evidence

A firm's users can access only the matters they have permission to see. LegalPrizm also has access. LegalPrizm operates the service and administers the encryption keys, so authorized LegalPrizm personnel are able to access a firm's data while monitoring and maintaining the service.

LegalPrizm restricts that access to authorized personnel who are subject to confidentiality obligations. LegalPrizm does not use case material for independent product improvement or model training. Review of case material for any purpose beyond providing the authorized service requires separate documented authorization from the firm.

Counsel should treat LegalPrizm as a recipient of protected material. If the order limits who may receive that material, or requires each recipient to sign an acknowledgment, tell LegalPrizm before upload so that those steps can be completed first. Amazon Web Services hosts the service. The sub-processors page lists it and the other providers.

## Questions courts are asking about AI tools

Courts have begun writing AI terms into protective orders. In March 2026, federal courts in Colorado (*Morgan v. V2X, Inc.*) and Kansas (*Jeffries v. Harcros Chemicals, Inc.*) amended protective orders to limit which AI tools may receive discovery material. Orders of this kind ask whether a tool is open to the public, whether the provider may train on what it receives, whether the provider may pass material on, and whether the material can be deleted. LegalPrizm's answers for its hosted service are these.

- **Open or closed.** LegalPrizm is not a public AI tool. Access is limited to the firm's authorized users and the LegalPrizm personnel described above.
- **Training.** LegalPrizm does not use case material for independent product improvement or model training.
- **Passing material on.** The providers that can process evidence are listed on the sub-processors page. Customers covered by the Data Processing Agreement receive at least 30 days' notice before a provider is added or replaced.
- **Deletion.** A firm may direct return or deletion at the end of the service. The instruction covers originals, page text, search indexes, vectors and other matter derivatives under LegalPrizm's control. Backups expire on the schedule in the firm's agreement. The firm may request written confirmation of destruction.

These terms are in the Data Processing Agreement, which applies when it is part of the firm's service agreement. Confirm that it is. The order itself decides whether a tool may be used. These answers do not.

## California attorneys: Senate Bill 574

California Senate Bill 574 (Chapter 858, Statutes of 2026) was signed on September 30, 2026 and takes effect on January 1, 2027. It adds section 6068.1 to the Business and Professions Code and amends section 128.7 of the Code of Civil Procedure. An attorney who uses generative AI to assist in the practice of law must do the following.

- Keep the practice of law with the attorney. The statute says an attorney "shall not delegate the practice of law to generative artificial intelligence."
- Keep confidential, personal identifying and other nonpublic information out of a generative AI system, unless access to the system is restricted to the attorney and to persons the attorney has authorized who are obligated to protect the information's confidentiality.
- Take reasonable steps to verify the accuracy of generative AI output, including all case and statutory citations, and to correct erroneous or hallucinated output in any material the attorney uses.
- Disclose the use of generative AI to the court for all documents submitted to the court.

- Consider whether to disclose the use of generative AI when it creates content provided to the public.

Separately, a paper filed in court may not contain citations that the attorney responsible for submitting it has not personally verified, whatever their source.

The statute defines generative AI as an AI system that can generate derived synthetic content, such as text, images, video and audio, that emulates its training data. The embedding and extractive models in the reviewed workflow rank and select passages that already exist in the evidence. They do not write new text. Whether a tool falls within the statute is a question for counsel.

If a firm authorizes a generative model through Amazon Bedrock, the attorney's duties under SB 574 apply to that use. The LegalPrizm personnel described above would be among the persons with access, so counsel should confirm that their authorization and confidentiality obligations satisfy the statute. The answer view links each passage to its source so that a reviewer can check the original page.

### Retention and provider terms

The reviewed workflow retains evidence, searchable text and indexes for review. Local processing alone does not establish zero retention. Where an order requires confidentiality terms, restrictions on disclosure or model training, or deletion of originals and derivatives, counsel should confirm those terms and the applicable retention and deletion procedures in writing for the specific deployment. The deployment record and the firm's agreement identify the processing locations, retention periods and recovery targets that apply. Firms may contact LegalPrizm to review these questions before submitting protected material.

### Compliance status and hosting

LegalPrizm's goal is to operate at the level of SOC 2 controls. LegalPrizm has not been independently verified as SOC 2 compliant and does not hold a SOC 2 report at this time.

LegalPrizm runs on Amazon Web Services. AWS reports that independent auditors assess its services under programs that include SOC 1, SOC 2 and SOC 3, and ISO/IEC 27001, 27017 and 27018. Those reports describe AWS's own controls. They do not cover LegalPrizm's software or operations. AWS lists these at aws.amazon.com/compliance/programs.

LegalPrizm will use AWS Regions on the US East Coast and the US West Coast, and will place the system in two Availability Zones. The same stack serves shared and private hosting. On shared hosting, several firms use one environment. On private hosting, the environment serves one firm only.

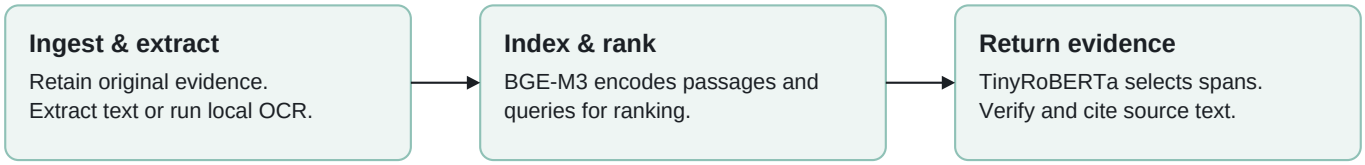
**/s/ Gene Avakyan, CEO** · November 28, 2026 · Revised November 29, 2026
Gene Avakyan, Chief Executive Officer, LegalPrizm

# How evidence moves through LegalPrizm

Local evidence processing and the AWS production architecture. Written for the firm's IT staff and litigation support vendors.

## Reviewed local workflow

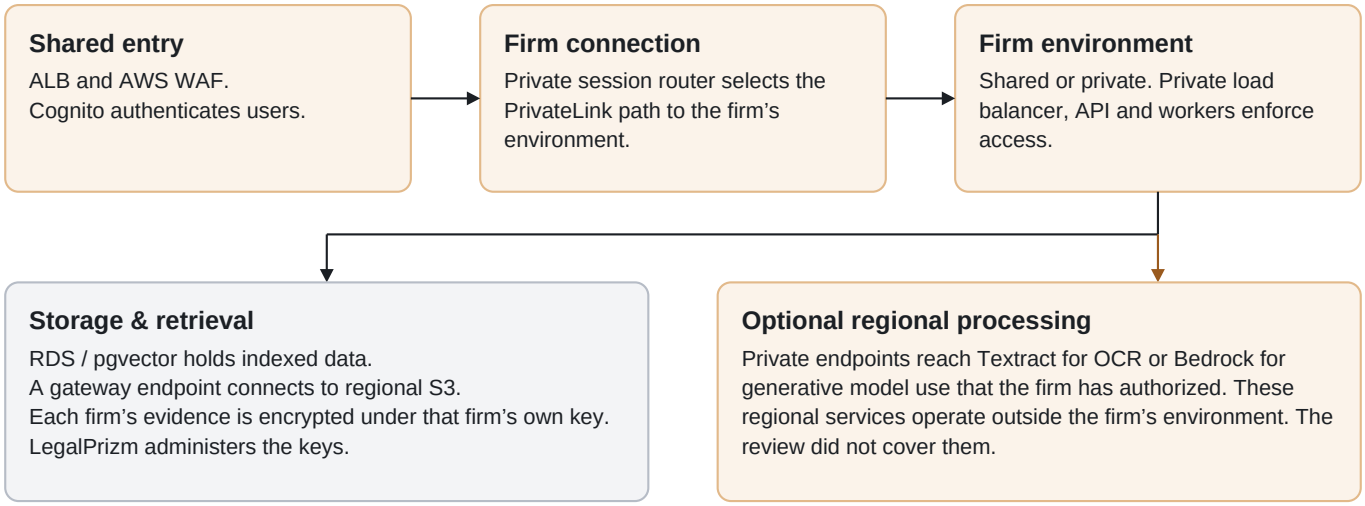
Evidence stays within the reviewed local processing and retrieval path.




Keyword search can retrieve passages directly. Semantic search and extractive answers use local models. Originals, searchable text and indexes persist so authorized reviewers can revisit the evidence. LegalPrizm conducted this review itself on November 28, 2026.

## AWS architecture

The same stack serves shared and private hosting. On shared hosting, several firms use one environment. On private hosting, the environment serves one firm only. The November 28 review covered the local processing and retrieval workflow.




LegalPrizm will use AWS Regions on the US East Coast and the US West Coast, and will place the system in two Availability Zones.

### Safeguards for either deployment

Check the operative order and amendments before enabling each service or model. Limit access by firm and matter. Apply required consent, provider terms, retention, legal holds and deletion controls to originals and derivatives. Verify the deployed configuration before using protected material.


LegalPrizm is a dba of VUGA Enterprises LLC, part of VUGA Group.
18117 Biscayne Blvd Unit 1039, Aventura, FL 33160, United States