> ⚠ ***DRAFT*** *— Automatically generated working document. Not a recognised conformity assessment under Regulation (EU) 2024/1689 Art. 11/47. Must be reviewed by qualified legal counsel before submission to any authority or Notified Body. Scanara accepts no liability for regulatory use of this document.*

Justice App - Post-Market Monitoring Plan (Art. 72)

Organisation: —
AI System: Justice App
Risk Level: high_risk
Version: 1
Generated: 2026-07-02 21:32:08.924232+00:00

Table of Contents

Post-Market Monitoring Strategy 3
Monitoring Strategy 3
Performance Metrics and Thresholds 4
Performance Metrics and Thresholds 4
Incident Reporting Procedures 5
Incident Reporting Procedures 5
Corrective Action Protocol 6
Corrective Action Protocol 6
Data Collection Methods 7
Data Collection Methods 7
Responsible Persons 8
Responsible Persons 8
Review Schedule 9
Review Schedule 9

Post-Market Monitoring Strategy

Monitoring Strategy

This section describes the post-market monitoring strategy for the AI system in accordance with Article 72 of the EU AI Act.

Monitoring Objectives

Verify that CaseInsight's sentencing-outcome prediction and evidence-reliability scoring continue to perform within declared accuracy and fairness parameters throughout deployment, and detect emerging automation-bias patterns in judicial usage.

Scope of Monitoring

Prediction accuracy, evidence-reliability calibration, demographic fairness (disparate impact), judge override behaviour, and input data drift.

Monitoring Methodology

Automated collection of prediction logs, confidence scores, and override records; quarterly statistical review by the compliance team; downstream reconciliation of predicted outcomes against actual case outcomes and appeal results where available.

Regulatory Basis

This post-market monitoring plan is established pursuant to Article 72 of Regulation (EU) 2024/1689 (EU AI Act). The provider shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the AI system and the risks involved.

Performance Metrics and Thresholds

Performance Metrics and Thresholds

This section defines the key performance indicators and acceptable thresholds for the AI system.

Key Performance Indicators

Metrics are tracked separately for sentencing-outcome prediction and evidence-reliability scoring, with fairness assessed across both.

Metric	Target	Threshold	Measurement Method
Accuracy	≥ 85%	< 80% triggers review	Multi-class accuracy vs. actual court outcome
Precision	≥ 85% (evidence-reliability)	< 80% triggers review	vs. expert-reviewer labels
Recall	≥ 85% (evidence-reliability)	< 80% triggers review	vs. expert-reviewer labels
Fairness	Disparate impact ratio 0.8–1.25	Outside range triggers review	Demographic-stratified accuracy comparison

Acceptable Thresholds

A sustained accuracy drop of more than 5 percentage points from baseline, or a disparate-impact ratio outside 0.8–1.25 for two consecutive quarters, triggers mandatory review under the Corrective Action Protocol.

Drift Detection

Quarterly comparison of input feature distributions (offence type, jurisdiction mix) against the training baseline using population stability index. Evidence-reliability score distribution is monitored monthly for calibration drift exceeding 10%.

Incident Reporting Procedures

Incident Reporting Procedures

This section documents the procedures for reporting and handling incidents related to the AI system, in line with Article 73 of the EU AI Act.

Incident Definition

A serious incident (Art. 3(49)) includes any systematic pattern of demonstrably discriminatory sentencing recommendations, a malfunction that materially affected an actual judicial outcome, or a confirmed data breach involving case data.

Reporting Channels

Judges, clerks, and IT staff report suspected incidents via Example Regional Court Administration's internal compliance channel, escalated immediately to Example AI Systems Ltd.'s compliance officer.

Reporting Timelines

In accordance with Article 73, providers shall report serious incidents to the market surveillance authorities of the Member States where the incident occurred: - **Initial report:** within 15 days of becoming aware of the serious incident - **Interim report:** within 30 days (if initial report is incomplete) - **Final report:** within 90 days

Internal Escalation

The compliance officer triages within 24 hours; critical incidents (active fundamental-rights harm risk) are escalated same-day to Example AI Systems Ltd.'s designated AI Act compliance lead and to Example Regional Court Administration's data protection officer.

Corrective Action Protocol

Corrective Action Protocol

This section describes the procedures for implementing corrective actions when performance issues or incidents are identified.

Trigger Conditions

Breach of the accuracy or fairness thresholds defined in Performance Metrics and Thresholds; any confirmed serious incident; or a formal request from a market surveillance authority.

Corrective Action Types

Corrective actions are selected proportionate to severity; all of the following are available to Example AI Systems Ltd.:

Possible corrective actions include: - System retraining or recalibration - Modification of input data requirements - Update of human oversight procedures - Temporary restriction or suspension of the system - Recall or withdrawal from the market

Implementation Process

Severity triage → root-cause analysis (data issue, model drift, or code defect) → fix (retraining, threshold adjustment, or code correction) → re-validation against the thresholds in Performance Metrics and Thresholds → documentation update (Annex IV, and the FRIA where fundamental-rights impact is implicated) → redeployment approval by the compliance officer.

Communication to Deployers

Example Regional Court Administration's designated contact is notified in writing within 5 working days of any corrective action affecting system availability or output reliability, with a summary suitable for internal court communication.

Data Collection Methods

Data Collection Methods

This section describes how data is collected for post-market monitoring purposes.

Data Sources

System prediction and evidence-scoring logs, judge override records with stated reasons (once mandatory capture is implemented), and downstream case-outcome/appeal data reconciled from the court case-management system.

Collection Frequency

Continuous automated log collection; quarterly manual reconciliation against case outcomes.

Data Processing and Storage

Monitoring data is stored in the same append-only, access-restricted storage as operational logs (see Annex IV, Record-Keeping, Logging and Retention). Demographic metadata used for fairness monitoring is processed on a minimised basis under the lawful basis established in the system's DPIA and is not used in individual case predictions.

Feedback from Deployers and Users

Example Regional Court Administration's designated liaison submits quarterly qualitative feedback from judges and clerks alongside the compliance team's quantitative review.

Responsible Persons

Responsible Persons

This section identifies the persons responsible for post-market monitoring activities.

PMM Plan Owner

Role	Name	Contact
PMM Plan Owner	*[To be completed by the provider — name of the individual accountable for this PMM Plan]*	*[work email]*

Monitoring Team

The compliance team at Example AI Systems Ltd. is responsible for day-to-day monitoring activities described in this plan, including quarterly performance review, drift detection, and reconciliation against case outcomes. *[To be completed by the provider — name the specific individuals or roles on this team]*

Incident Response Lead

[To be completed by the provider — name of the individual who owns Art. 73 serious-incident triage and reporting, referenced in Incident Reporting Procedures]

Provider Contact

Field	Details
Organisation	Example AI Systems Ltd.
Contact	*[To be completed — this and the fields above are seeded from your org profile's `legal_name` /contact fields plus a dedicated PMM `plan_owner` / `monitoring_team` / `incident_response_lead` form; the org profile alone won't populate the PMM-specific roles]*
Email	*[To be completed]*

Review Schedule

Review Schedule

This section defines the schedule for regular reviews of the post-market monitoring plan and the AI system's compliance status.

Review Frequency

Recommended minimum review intervals: - **Quarterly:** Performance metrics and threshold compliance (see Performance Metrics and Thresholds) - **Semi-annually:** Full system review including bias and drift assessment across demographic groups - **Annually:** Comprehensive review of the entire PMM plan, aligned with AIRA/FRIA renewal

Review Scope

Quarterly reviews cover accuracy, override-rate, and drift metrics. Semi-annual and annual reviews additionally cover incident history, corrective actions taken, and any changes to deployment context.

Review Outcomes and Documentation

Findings are documented in a review report retained under the same record-keeping obligations as operational logs (10-year retention). Material findings trigger an update to this PMM Plan and, where applicable, the Annex IV Technical Documentation.

Next Scheduled Review

[To be set at dossier finalisation — first quarterly review due 3 months after go-live]

Disclaimer

This document was automatically generated by the Scanara platform. It is provided as a compliance aid under Regulation (EU) 2024/1689 (EU AI Act) and does not constitute legal advice. Organisations are responsible for ensuring accuracy and completeness.