EU AI ACT · PAYMENT OPERATORS · AUGUST 2026

EU AI Act Compliance Checklist

A 47-point readiness checklist for PSPs, iGaming operators, and fintech companies using automated fraud detection systems. Covers Article 13 transparency, audit trail, documentation, and operational requirements before the August 2026 enforcement date.

Enforcement date: August 2026	**Non-compliance fine ceiling:** 7% of global annual turnover	**Applies to:** Any operator using automated decision-making in fraud detection

SECTION A — Article 13: Transparency & Explainability

12 requirements

- [ ] A1 **Per-decision explainability log exists**
  Every automated fraud decision must have a human-readable rationale recorded at the time of decision.
- [ ] A2 **Explainability log is human-readable**
  The log must be interpretable by a non-technical compliance officer — not just raw model scores.
- [ ] A3 **Explainability log is timestamped and immutable**
  Log entries cannot be modified after creation. Timestamp must be accurate to the second.
- [ ] A4 **Explainability log is exportable on demand**
  You can produce the full log for a regulatory inspection within a defined SLA (target: under 45 minutes).
- [ ] A5 **Log covers all automated decisions — not only declines**
  Article 13 applies to all automated decisions in the fraud detection pipeline, including approvals and flag-for-review.
- [ ] A6 **Model version is recorded per decision**
  Each log entry references the model version that produced the decision.
- [ ] A7 **Input features used per decision are recorded**
  The specific signals that influenced each decision must be logged — not just the final score.
- [ ] A8 **Confidence/score range is documented alongside decision**
  The numerical score and its interpretation (high/medium/low risk) must be recorded.
- [ ] A9 **Human override path exists and is documented**
  Operators must be able to override automated decisions. The override path must be documented and logged.
- [ ] A10 **Transparency notice published for affected parties**
  If automated decisions affect individuals (e.g. transaction declines), a transparency notice must be accessible.
- [ ] A11 **Right to explanation is operationalised**
  Individuals affected by automated decisions have the right to request an explanation. A process for handling these requests must exist.
- [ ] A12 **Audit log is accessible to relevant regulators**
  Regulators (FCA, BaFin, DNB, etc.) must be able to access audit logs on request. Access procedure is documented.

SECTION B — Technical Documentation & Model Governance

10 requirements

B1	☐	**Technical documentation for the AI system exists** A document describing the system's purpose, design, capabilities, and limitations must exist before deployment.
B2	☐	**Risk management framework documented** The risk management approach for the AI system is documented and maintained.
B3	☐	**Training data documentation exists** Information about the data used to train the model — sources, preprocessing, labelling — must be documented.
B4	☐	**Model performance metrics are documented and monitored** Precision, recall, false positive rate, and drift metrics are tracked and available.
B5	☐	**Model retraining schedule and trigger conditions are defined** When and why the model is retrained must be documented. Drift thresholds trigger retraining.
B6	☐	**Accuracy and error rates are validated on relevant population** Model performance must be validated specifically on your transaction population — not just general benchmarks.
B7	☐	**Bias and fairness assessment completed** The model has been assessed for discriminatory patterns across protected characteristics.
B8	☐	**Known limitations are documented** The documentation must honestly state what the system cannot do — not just what it can.
B9	☐	**Version control for model and documentation** Every model version and its associated documentation is versioned and accessible.
B10	☐	**Post-market monitoring plan exists** A plan for ongoing monitoring of the system after deployment is documented.

SECTION C — Operational Readiness

10 requirements

C1	☐	**Human oversight mechanism is in place** A human-in-the-loop review process exists for high-risk or ambiguous decisions.
C2	☐	**Escalation path for edge cases is defined** When the system flags a decision for review, the routing path to human analysts is defined and tested.
C3	☐	**Operator-configurable risk thresholds exist** Risk operations teams can adjust decision thresholds without requiring model retraining.
C4	☐	**Analyst feedback loop is implemented** Analyst review outcomes (correct/incorrect decision) feed back into the model to improve accuracy.
C5	☐	**Incident response procedure exists for model failures** If the AI system fails or produces erroneous decisions at scale, an incident response procedure is documented.

C6 ☐ **Downtime fallback procedure exists**
If the AI system becomes unavailable, a documented fallback procedure maintains fraud operations.

C7 ☐ **SLA for automated decision latency is defined**
The maximum acceptable response time for automated fraud decisions is defined and monitored.

C8 ☐ **Chargeback representment evidence is machine-generated**
Evidence packets for dispute representment are automatically assembled at detection time — not manually compiled.

C9 ☐ **Integration with card scheme dispute workflows**
The system integrates with Visa/Mastercard dispute resolution workflows or can export evidence in required formats.

C10 ☐ **Regulatory export SLA is defined and tested**
The SLA for producing a compliance export (e.g. for audit purposes) is defined and has been tested end-to-end.

SECTION D — Data Governance & Privacy

8 requirements

D1 ☐ **All transaction data processed within EU data centres**
No personal or transaction data leaves the EU. GDPR Article 44 transfer rules satisfied.

D2 ☐ **Data retention periods are defined and enforced**
Retention periods for transaction data, model inputs, and audit logs are documented and technically enforced.

D3 ☐ **Data minimisation principle applied**
Only the data necessary for fraud detection is collected and processed.

D4 ☐ **Data subject rights are operationalised**
Processes exist for handling access, rectification, erasure, and portability requests.

D5 ☐ **Third-party data processors are assessed**
Any third party processing transaction data on your behalf has been assessed for compliance.

D6 ☐ **Data processing agreement (DPA) in place with all processors**
A GDPR-compliant DPA is in place with all vendors processing personal data.

D7 ☐ **Pseudonymisation or anonymisation applied where possible**
Data used for model training and evaluation is pseudonymised where possible.

D8 ☐ **Data breach response procedure exists**
A documented procedure for detecting, reporting, and responding to data breaches is in place.

SECTION E — Regulatory Reporting & Compliance Documentation

7 requirements

E1 ☐ **EU AI Act Article 13 compliance statement prepared**
A written statement confirming the system's compliance with Article 13 transparency requirements.

E2	☐	**Compliance documentation is regulator-ready** All documentation is in a format that can be submitted directly to a regulator without reformatting.
E3	☐	**VAMP threshold monitoring is in place** Visa Advanced Monitoring Programme threshold (0.9%) is tracked monthly. Alert procedure exists if threshold approached.
E4	☐	**Card scheme dispute ratio is tracked** Mastercard Excessive Chargeback Programme and Visa Dispute Monitoring Programme ratios are tracked and reported.
E5	☐	**Board-level awareness of EU AI Act obligations confirmed** Board or senior management has been briefed on EU AI Act obligations and has approved the compliance approach.
E6	☐	**Legal counsel has reviewed AI system documentation** Qualified legal counsel has reviewed the technical documentation and compliance statements.
E7	☐	**Compliance review cadence is scheduled** A recurring review of the AI system's compliance status is scheduled — at minimum, annually.

Your compliance baseline — starting now

The fastest path to an EU AI Act audit trail is a 50-day shadow mode evaluation with SENTR. During the evaluation, SENTR generates a full explainability log for every fraud decision — human-readable, regulator-ready, and exportable in under 45 minutes. You don't need to be live on SENTR before August 2026. You need to demonstrate you are building toward compliance.

Book a 20-minute Architecture Session at sentr.io/proof

This checklist is for informational purposes only. It does not constitute legal advice. Consult qualified legal counsel to assess your organisation's specific obligations under the EU AI Act. Regulatory requirements are subject to change — verify all claims against current EUR-Lex publications.