

EU AI Act — Article 13

Transparency

EU AI Act Art. 13

If you place a high-risk AI system on the EU market, you must give deployers enough information to use it safely and lawfully. This pack turns that obligation into a checklist your auditor can sign.

AUTHORITY	European Union (European Parliament and Council)
PUBLICATION	Regulation (EU) 2024/1689
VERSION	1.0.0 · License: Apache-2.0
URL	https://eur-lex.europa.eu/eli/reg/2024/1689/oj

About this pack

This is the EU AI Act Art. 13 pack from the AIGovOps Beacon audit framework. Walk it with your auditor, your CISO, and the engineer who actually ships the system. It is short on purpose.

Items marked **auto** are computed by Beacon from signed receipts and the model inventory — you do not have to hand-evidence them, the platform does. Items without that badge require a human attestation: a person reads the prompt, checks the evidence is real, and ticks a box. Beacon records the attestation as a signed receipt with `event_type attestation`.

The severity label tells you how much weight an item carries in the production-readiness gate. Critical items can fail a release on their own. Lower-severity items contribute to a weighted score.

This pack is released under the Apache License 2.0. The underlying source publication retains its own copyright; consult it for normative language.

Checklist — Functions

ART13-INSTRUCTIONS

Instructions for use

Art. 13(2) and 13(3)(a–b). Information accompanying the system.

ART13-1.1

CRITICAL

Are instructions for use provided in a digital format accessible to deployers?

Evidence `instructions_uri` Gate `instructions_published`

☐ Yes ☐ No ☐ N/A

ART13-1.2

HIGH

Do the instructions identify the provider and, where applicable, the authorized representative?

Evidence `provider_identity_doc`

☐ Yes ☐ No ☐ N/A

ART13-1.3

HIGH

Are the instructions concise, complete, correct, clear, relevant, accessible, and comprehensible to deployers? (Art. 13(2))

Evidence instructions_review_signoff

☐ Yes ☐ No ☐ N/A

ART13-CHARACTERISTICS

Characteristics, capabilities, and limitations

Art. 13(3)(b)(i-v).

ART13-2.1

CRITICAL

Is the intended purpose documented, including foreseeable misuse?

Evidence intended_purpose_doc Gate intended_purpose_present

☐ Yes ☐ No ☐ N/A

ART13-2.2

CRITICAL

Are levels of accuracy, robustness, and cybersecurity declared, with the metrics used to measure them?

Evidence performance_declaration

☐ Yes ☐ No ☐ N/A

ART13-2.3

CRITICAL

Are foreseeable circumstances that may lead to risks to health, safety, or fundamental rights described?

Evidence risk_circumstances_doc

☐ Yes ☐ No ☐ N/A

ART13-2.4

HIGH

Are the technical capabilities and characteristics relevant to explaining outputs described?

Evidence explainability_doc

☐ Yes ☐ No ☐ N/A

ART13-2.5

HIGH

Where relevant, is performance for specific persons or groups disclosed?

Evidence subgroup_performance_doc

☐ Yes ☐ No ☐ N/A

ART13-2.6

HIGH

Are the input data specifications (training/validation/testing) described, including provenance and any biases?

Evidence data_specs_doc

☐ Yes ☐ No ☐ N/A

ART13-2.7

HIGH

Is information provided that enables deployers to interpret outputs and use them appropriately?

Evidence interpretation_guidance_doc

☐ Yes ☐ No ☐ N/A

ART13-OVERSIGHT

Human oversight measures

Art. 13(3)(d) — measures referred to in Art. 14.

ART13-3.1

CRITICAL

Are the human oversight measures referenced in Art. 14 described, including technical measures to facilitate interpretation of outputs?

Evidence oversight_measures_doc Gate human_oversight_defined

☐ Yes ☐ No ☐ N/A

ART13-3.2

MEDIUM

Is the expected lifetime of the system stated, with any necessary maintenance and care measures?

Evidence lifecycle_doc

☐ Yes ☐ No ☐ N/A

ART13-LOGGING

Logging and traceability

Art. 13(3)(f) and cross-reference to Art. 12.

ART13-4.1

CRITICAL

AUTO

Is automatic logging of events enabled for the lifetime of the system? (Art. 12)

Evidence beacon_receipts_active Gate receipts_captured

☐ Yes ☐ No ☐ N/A

ART13-4.2

CRITICAL

Are logs kept for the period required by Union or national law, and at least six months unless otherwise specified?

Evidence retention_policy_uri Gate retention_minimum_6mo

☐ Yes ☐ No ☐ N/A

ART13-4.3

HIGH

AUTO

Is there a mechanism for deployers to collect, retain, and analyze the logs?

Evidence beacon_export_endpoint Gate export_endpoint_present

☐ Yes ☐ No ☐ N/A

ART13-POSTMARKET

Post-market information

Information that must remain current after deployment.

ART13-5.1

HIGH

Is there a process to update instructions when the system or its risks materially change?

Evidence change_management_uri

☐ Yes ☐ No ☐ N/A

ART13-5.2

HIGH

Are deployers notified of material changes within a defined SLA?

Evidence deployer_notification_log

☐ Yes ☐ No ☐ N/A

ART13-5.3

MEDIUM

Is contact information for the provider's post-market monitoring function published and tested?

Evidence contact_uri

☐ Yes ☐ No ☐ N/A

Scoring

How Beacon scores this pack:

- All items default to attestation unless `auto_check: true`.
- PASS threshold defaults to 0.95 for `high_risk_systems` (configurable).
- Failure on any "critical" item sets `gate.eu_ai_act = FAIL`.