



INDICATIVE REGULATORY SELF-ASSESSMENT

EU AI Act Report

Regulation (EU) 2024/1689, as amended by Regulation (EU) 2026/1744 ("Digital Omnibus")

PREPARED FOR

Maison Orée

Claire Martin contact@maison-oree.example

RISK CLASSIFICATION

● Characteristics associated with high risk

INDICATIVE SCORE

33 / 100

PUBLISHED BY EUAICheck (Vival Solutions EI)

ORGANISATION Maison Orée

CONTACT contact@maison-oree.example

LEGAL FRAMEWORK Regulation (EU) 2024/1689, Article 6 and Annexes I and III, as amended by Regulation (EU) 2026/1744

Self-assessment tool, not legal advice. This report relies solely on your declarations. It is neither an audit nor a certification. Drafted with the help of generative AI (Anthropic), constrained by rules and excerpts of the official text; references checked on 27/09/2026. For legal advice, consult a specialised lawyer.

CONTENTS

Table of contents

01	Executive summary	3
02	Your system and your declaration	4
03	Risk level and legal basis	5
04	Use context	5
05	Applicable articles matrix	6
06	Compliance analysis — score and vectors	7
07	Detailed gap analysis	8
08	Prioritised action plan	10
09	Personalised regulatory timeline	12
10	Penalty exposure	13
11	What a formal audit involves	13
12	Recommendation and next steps	14
13	Glossary	15
14	Reference texts	17

ABOUT THIS REPORT

EUAICheck is an independent self-assessment tool. This report highlights points of attention based on your answers and helps prioritise. It replaces neither a specialised lawyer's advice nor a conformity assessment by a notified body where the Regulation requires one.

This report was generated automatically from your answers: classification follows fixed rules, obligations are described from the text of the Regulation, and drafted parts are produced by generative AI (Anthropic) without sending your name, email or company. Reference: Regulation (EU) 2024/1689, as amended by Regulation (EU) 2026/1744 ("Digital Omnibus"), checked on 27/09/2026.

01 EXECUTIVE SUMMARY

Your situation at a glance

RISK CLASSIFICATION

● Characteristics associated with high risk

33%

INDICATIVE SCORE

4

ACTION POINTS

2

COMPLIANT VECTORS

SUMMARY

Based on your answers, your tool pre-screens the job applications received for your shops and influences hiring decisions: it shows characteristics associated with high risk (Annex III, point 4, employment). You use it as the deployer of a tool bought from a vendor. Human oversight and the allocation of roles are in place; documentation of input data, logging, informing candidates and risk assessment still need work. This level is indicative and based solely on your answers.

KEY GAPS IDENTIFIED

Art. 10 (provider) · Art. 26(4) (deployer)	Data documentation and governance	Action required
Art. 12 · Art. 19 · Art. 26(6)	Logging and traceability	Action required
Art. 26(11) · Art. 86	Information and explanation to affected persons	Action required
Art. 9 (provider) · Art. 26(5) and 27 (deployer)	Risk management	Action required

Each gap is detailed in section 07 (obligation, risk, action); the prioritised action plan is in section 08.

02 YOUR SYSTEM AND YOUR DECLARATION

What you declared to us

This document is based on information declared by Claire Martin on behalf of Maison Orée on 04/10/2026. These declarations constitute the exclusive basis of the analysis.

SYSTEM DESCRIPTION

"Our tool screens the job applications we receive for our shops"

— Claire Martin, Maison Orée

DECLARED ANSWERS BY VECTOR

COMPLIANCE VECTOR	ARTICLE	STATUS
Data documentation	Art. 10 · 26(4)	Action required
Effective human oversight	Art. 14 · 26(2)	In place
Logging & traceability	Art. 12 · 26(6)	Action required
Information & explanation	Art. 26(11) · 86	Action required
Roles & competence	Art. 4 · 17 · 26	In place
Risk management	Art. 9 · 27	Action required

03 RISK LEVEL AND LEGAL BASIS

Why this classification

CHARACTERISTICS ASSOCIATED WITH HIGH RISK

The Regulation lists among high-risk uses AI systems intended for the recruitment or selection of people, in particular to filter or evaluate applications (Annex III, point 4). Your tool, which sorts applications before a recruiter reviews them, matches this description. As a deployer, your main obligations are in Article 26: use the system in accordance with its instructions, assign human oversight to competent people, ensure the relevance of the input data you control, keep the logs and inform the persons concerned. Regulation (EU) 2026/1744 set these obligations to apply from 2 December 2027; since your tool is already in production, the remaining fourteen months are the right time to prepare.

04 USE CONTEXT

The EU AI Act for this type of use

Recruitment is one of the most regulated uses of AI in the Regulation, because the result can directly change a person's situation. For an SME using a vendor's tool, the most common practical difficulties are obtaining usable instructions for use and documentation from the vendor, tracing the results produced so they can be explained, and clearly informing candidates that AI is used to process their application.

COMMON GAPS FOR THIS TYPE OF USE

- 1 No bias testing on data
- 2 Candidates or employees not informed of AI use
- 3 No explanation or human review channel
- 4 Informal or insufficient human oversight

05 APPLICABLE ARTICLES MATRIX

Articles associated with your answers

The table below indicates, for each relevant article of the Regulation, whether it is associated with the characteristics you declared. Several obligations differ depending on whether you are the provider or the deployer of the system.

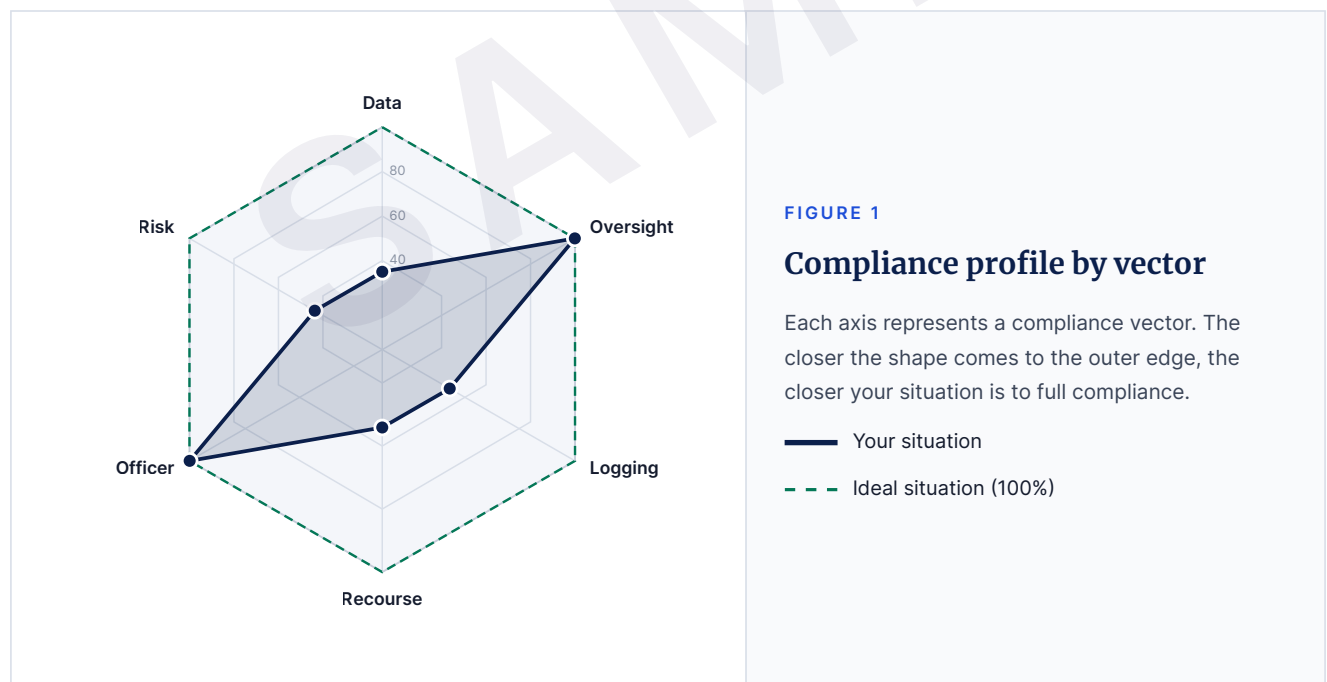
ARTICLE	SUBJECT	APPLICABLE	NOTE
Art. 4	AI literacy	Yes	Measures to support AI literacy of staff, for all providers and deployers.
Art. 5	Prohibited practices	No	Based on your answers, no characteristic of a prohibited practice was identified.
Art. 6	High-risk classification	Yes	Your answers show characteristics associated with Annex III or Annex I.
Art. 9	Risk management	Yes	Provider obligation.
Art. 10	Data and data governance	Yes	Provider obligation; the deployer ensures input data relevance (Art. 26).
Art. 11	Technical documentation	Yes	Provider obligation, content set out in Annex IV.
Art. 12	Record-keeping	Yes	Automatic logging; deployer retention of at least six months (Art. 26).
Art. 13	Transparency and instructions for use	Yes	The provider gives the deployer clear instructions on capabilities and limitations.
Art. 14	Human oversight	Yes	Design enabling effective human oversight.
Art. 15	Accuracy, robustness, cybersecurity	Yes	Provider obligation.
Art. 17	Quality management system	Yes	Provider obligation, lighter for SMEs.
Art. 26	Deployer obligations	Yes	Use per instructions, human oversight, input data, logs, informing persons.
Art. 27	Fundamental rights impact assessment	Partial	For certain deployers (public bodies, public services, Annex III points 5(b) and (c)).
Art. 49	Registration in the EU database	Yes	By the provider before placing on the market; also by certain public deployers.
Art. 50	Transparency towards persons	Partial	If the system interacts with people or generates content.
Art. 86	Right to explanation	Yes	For individual decisions based on an Annex III system.

06 COMPLIANCE ANALYSIS

Your score breakdown

Your indicative score is 33%: two of the six areas are fully in place, human oversight and the allocation of roles. The other four are partly in place. For an application-screening tool, the most useful areas to strengthen are logging, which lets you explain a contested result, and informing candidates, which GDPR already expects before the high-risk obligations apply.

VECTOR	LEVEL	IN PLACE	STATUS
Data documentation Art. 10 · 26(4)		Partial	Action required
Effective human oversight Art. 14 · 26(2)		In place	In place
Logging & traceability Art. 12 · 26(6)		Partial	Action required
Information & explanation Art. 26(11) · 86		Partial	Action required
Roles & competence Art. 4 · 17 · 26		In place	In place
Risk management Art. 9 · 27		Partial	Action required



07 DETAILED GAP ANALYSIS

Your gaps – obligations and actions

For each point of attention, you will find below what the Regulation provides, why it matters, and an indicative action.

Art. 10 (provider) · Art. 26(4) (deployer)	Data documentation and governance	ACTION REQUIRED
OBLIGATION	For a high-risk system, the provider applies governance practices to training, validation and testing datasets: design choices, data origin and collection, preparation, assumptions, examination of possible biases and measures to detect and mitigate them (Article 10). The deployer, to the extent it controls input data, ensures that data is relevant and sufficiently representative in view of the system's intended purpose (Article 26(4)).	
WHY IT MATTERS	Without available documentation, demonstrating compliance during a market surveillance check is difficult. Non-compliance with operator obligations falls under the ceiling of Article 99(4).	
ACTION	Build a data register: origin, collection conditions, selection criteria, pre-processing, bias analysis and corrective measures, dataset versions. For a purchased system, request the provider's documentation and document your own input data.	

Art. 12 · Art. 19 · Art. 26(6)	Logging and traceability	ACTION REQUIRED
OBLIGATION	High-risk systems technically allow automatic recording of events (logs) over their lifetime (Article 12). The provider keeps logs under its control (Article 19). The deployer keeps logs under its control for a period appropriate to the intended purpose, of at least six months unless otherwise provided by applicable law (Article 26(6)).	
WHY IT MATTERS	Without logs, a contested decision or an incident cannot be reconstructed, which makes answering an authority or an affected person difficult.	
ACTION	Implement automatic logging of each AI output: timestamp, input data (pseudonymised where possible), output produced, associated human validation. Retain logs for at least six months.	

Art. 26(11) - Art. 86	Information and explanation to affected persons	ACTION REQUIRED
OBLIGATION	A deployer of an Annex III system that makes or assists decisions related to natural persons informs them that they are subject to the use of the system (Article 26(11)). A person subject to a decision based on the output of such a system, with legal effects or similarly significant effects, has the right to obtain clear and meaningful explanations of the system's role in the decision (Article 86). Anyone may also lodge a complaint with a market surveillance authority (Article 85).	
WHY IT MATTERS	The Regulation does not itself require a formal contestation procedure, but without an information and explanation channel, requests under Article 86 cannot be answered. Where a decision is based solely on automated processing of personal data, GDPR Article 22 also grants the right to human intervention and to contest the decision.	
ACTION	Inform affected persons that the system is used; open a channel for explanation and human review requests, with a defined response time and a request register.	

Art. 9 (provider) - Art. 26(5) and 27 (deployer)	Risk management	ACTION REQUIRED
OBLIGATION	The provider of a high-risk system establishes, documents and maintains a risk management system over the whole lifecycle: identification and analysis of reasonably foreseeable risks to health, safety and fundamental rights, management measures and testing (Article 9). The deployer uses the system in accordance with the instructions for use, monitors its operation and informs the provider of risks (Article 26(5)). Certain deployers, notably public bodies, private entities providing public services and deployers of Annex III points 5(b) and 5(c), carry out a fundamental rights impact assessment (Article 27).	
WHY IT MATTERS	Without a written assessment, demonstrating that risks were identified and managed is difficult.	
ACTION	Conduct and document a risk assessment: data biases, error rates across affected groups, misuse scenarios, consequences of an error for people. Update it at each significant change to the system.	

08 PRIORITISED ACTION PLAN

Your next steps

Actions ranked by priority, personalised according to your gaps. Estimated effort and legal basis are indicated for each action.

1**Request the instructions for use and documentation from the vendor****D-30****EFFORT : LOW****WHAT**

Send the tool's vendor a written request: instructions for use, the data used to train the system, known limitations, recommended human oversight measures and the log format.

WHY

The deployer uses the system in accordance with the instructions for use (Article 26), which the provider must supply (Article 13).

2**Inform candidates that the tool is used****D-30****EFFORT : LOW****WHAT**

Add a clear notice to job ads and to the application acknowledgement: the tool used, its role in screening, and the option to ask for a review by a person.

WHY

The deployer informs persons that they are subject to the use of an Annex III system (Article 26(11)); right to an explanation (Article 86).

3**Set up log retention****D-30****EFFORT : MEDIUM****WHAT**

Check which logs the tool produces (date, application, result, recruiter decision) and keep them for at least six months.

WHY

Automatic logging (Article 12) and retention by the deployer of the logs under its control (Article 26(6)).

4**Document the input data****D-90****EFFORT : MEDIUM****WHAT**

Describe the information sent to the tool (CVs, cover letters, questionnaire answers), check that it is relevant for the positions concerned and remove unnecessary fields.

WHY

The deployer ensures the relevance of the input data it controls (Article 26(4)).

5 Write a one-page risk assessment

D-90

EFFORT : MEDIUM

WHAT	List the tool's possible errors (candidates wrongly rejected, bias by background), their consequences and the controls in place; review it with every new version.
WHY	Monitoring the system's operation and informing the provider of risks (Article 26(5)).

6 Train recruiters on the tool

D-180

EFFORT : LOW

WHAT	A short session for the people who validate results: what the tool does, its limits, and when and how to override its recommendation.
WHY	Measures to support AI literacy of staff (Article 4) and human oversight by competent people (Article 26(2)).

SAMPLE

09 PERSONALISED REGULATORY TIMELINE

Your personalised timeline

CURRENT SITUATION Based on your answers, your system is already in production. As of 04/10/2026: Articles 4, 5 and 50 apply; high-risk obligations are postponed by Regulation (EU) 2026/1744.



10 PENALTY EXPOSURE

Ceilings set by the Regulation

35 M€

Or 7% of global turnover - prohibited practices

15 M€

Or 3% of global turnover - other obligations

7,5 M€

Or 1% of global turnover - incorrect information. SMEs: the lower amount applies (Art. 99(6))

Failure to meet deployer obligations, including those of Article 26, can be fined up to 15 million euros or 3% of worldwide annual turnover (Article 99). For SMEs, the lower of the two amounts applies (Article 99(6)). Authorities consider the nature, gravity and duration of the infringement, the size of the company, its co-operation and the measures taken to mitigate harm (Article 99(7)): a documented compliance plan started before December 2027 counts in your favour. No fine estimate is given in this report.

11 WHAT A FORMAL AUDIT INVOLVES

After this report: the next step

A review by a specialised lawyer or consultant usually covers the contract with the vendor and the allocation of responsibilities, the instructions for use, how recruiters validate results, log retention, candidate information and the link with GDPR. Documents typically requested are the contract, the instructions for use, internal validation rules, a log extract and the information notices. This report is a starting point: it lists what to prepare so that the review focuses on what matters.

This EUAICheck report positions you for this next step. It constitutes your first structured self-assessment, identifies documents to prepare and gaps to fill before engaging a specialised lawyer (or, for certain regulated products, a notified body).

12 RECOMMENDATION AND NEXT STEPS

Our recommendation

EUAICHECK RECOMMENDATION

In the next thirty days, two actions matter most: ask the vendor for its instructions for use and documentation, and inform candidates that the tool is used. Both are simple and most other steps depend on them. Have this indicative classification confirmed by a specialised lawyer before any high-stakes decision.

PRACTICAL NEXT STEPS

#	ACTION	WHEN
1	Share this report with your management and legal counsel	This week
2	Inventory all AI systems used in your organisation	D-30
3	Prioritise the significant gaps identified in this report	D-30
4	Consult an AI law specialist for high-stakes points	D-60
5	Obtain the provider's documentation and instructions for use	D-90

13 GLOSSARY

Key EU AI Act terms

Definitions of technical and legal terms used in this report and in Regulation (EU) 2024/1689.

Deployer

Any person or organisation using an AI system under its authority in a professional context, whether developed in-house or purchased.

Provider

Any person or organisation that develops an AI system or has it developed and places it on the market or into service under its own name.

High-risk system

An AI system falling under Annex III, or a safety component of a regulated product listed in Annex I subject to third-party assessment.

Annex III

List of high-risk uses: biometrics, critical infrastructure, education, employment, essential services, law enforcement, migration, justice and democratic processes.

Article 4

Measures to support a sufficient level of AI literacy of staff, for all providers and deployers.

Article 5

List of AI practices prohibited in the EU, including manipulation, exploitation of vulnerabilities, social scoring, emotion recognition at work and in education.

Article 9

Provider risk management system over the lifecycle of a high-risk system.

Article 10

Governance requirements for training, validation and testing data (provider).

Article 12

Automatic event recording (logs) capability of high-risk systems.

Article 13

Provider transparency towards deployers: instructions for use, capabilities, limitations.

Article 14

Design enabling effective human oversight: understand, monitor, override an output, stop the system.

Article 17

Provider quality management system, proportionate for SMEs.

Article 26

Deployer obligations: use per instructions, human oversight, input data, log retention, informing persons.

Article 50

Transparency: inform people they interact with AI, mark generated content, disclose deepfakes.

Article 86

Right of an affected person to an explanation of an Annex III system's role in a decision concerning them.

GPAI (General Purpose AI)

AI model trained on large amounts of data and capable of many tasks (e.g. GPT, Claude, Gemini, Mistral).

Digital Omnibus

Regulation (EU) 2026/1744, published in the Official Journal on 24 July 2026 and in force since 27 July 2026; it postpones high-risk obligations to 2 December 2027 (Annex III) and 2 August 2028 (Annex I).

AI Office

European Commission service responsible notably for supervising general-purpose AI models.

FRIA

Fundamental rights impact assessment required from certain deployers of high-risk systems (Article 27).

Notified body

Designated third-party body performing certain conformity assessments.

CE marking

Marking affixed by the provider of a high-risk system after conformity assessment.

EUAICheck score

Educational indicator across 6 areas based on your self-declared answers. Not a certification or legal advice.

SAMPLE

14 REFERENCE TEXTS

Official reference texts

Official reference texts, freely available:

Regulation (EU) 2024/1689 on artificial intelligence

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

EUR-LEX

Regulation (EU) 2026/1744 ("Digital Omnibus"), amending it

<https://eur-lex.europa.eu/eli/reg/2026/1744/oj>

EUR-LEX

European Commission page on the AI regulatory framework (guidelines, FAQ)

<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

EUROPEAN COMMISSION

LEGAL NOTICE

This report is an educational tool generated by EUAICheck. It does not constitute legal advice within the meaning of French law of 31 December 1971, a compliance certification, or a regulatory guarantee. The information presented is based on the user's declarations and regulatory texts in force on 04/10/2026. For any high-stakes situation, consult a lawyer specialising in AI law. Drafted with AI assistance (Anthropic). Publisher: Vival Solutions (EI), SIRET 130 451 164 00011, Rochefort-du-Gard, France. Legal notice and terms: euaicheck.fr/mentions-legales and euaicheck.fr/conditions.



EUAICheck · euaicheck.fr · Rochefort-du-Gard, France
EUC-00000 · 04/10/2026