EASYLAB AI
RCS Luxembourg B276290 — TVA LU34756015
55 Rue de la Poudrerie, L-1899 Roeser

Easycore — Risk Assessment (FRIA)

Risk scenarios, mitigations and fundamental-rights screening — Edition 2026 · v2026.06 · Public

PURPOSE OF THIS DOCUMENT

This summary presents the principal risk scenarios of Easycore deployments, their technical and organisational mitigations, and the fundamental-rights screening, in the spirit of a FRIA. It is the public edition of the detailed assessment maintained for due diligence; risks are re-assessed per deployment during scoping.

1 Principal scenarios and mitigations

Scenario	Principal mitigations	Residual
Prompt injection via external content	External content processed as data, never instruction; isolated ephemeral sub-agents with restricted tools; multi-pattern sanitisation; injection resistance built into orchestration.	Low
Erroneous output released externally	Risk-level model: outbound outputs human-gated; red-level outputs nominative; drafts clearly marked.	Low
Confidentiality breach / data leak	Per-client isolation; EU hosting; loopback gateway and encrypted tunnels; single documented outbound flow; strong encryption for sensitive data.	Low
Behavioral drift over time	Independent Behavioral Trust Score every 6h across nine dimensions; automatic gate tightening and suspension on degraded bands.	Low
Runaway resource consumption	Per-agent budgets (tokens, calls, spend, human time) acting as circuit breakers.	Low
Provider / model dependency	LLM-agnostic ACP abstraction; substitutable runtime; documented exit strategy and data reversibility (DORA).	Managed

2 Fundamental-rights screening

- No Annex III use case is permitted on the platform (enforced by the Acceptable Use Policy): no credit scoring, no biometrics, no employment selection, no automated decisions with legal effect on persons.
- Human validation on any action materially affecting third parties is structurally enforced through gates.
- Worker impact: agents augment support functions; deployers receive an information-notice template; oversight roles are human by design.

Conclusion. Deployments within the intended-use envelope present limited risk to fundamental rights. The assessment is renewed per deployment and per material platform change; the detailed edition is available to clients and authorities in due diligence.

Easycore by Easylab AI — Public governance documentation, edition 2026 (v2026.06). Published for transparency and due-diligence purposes under Regulation (EU) 2024/1689. This document describes compliance by design and does not constitute legal advice. It reflects the state of the platform at the date of edition. Due-diligence inquiries: contact@easylab.ai — easycore.ai/governance