

COSMIC BROKKOLI

BUILD INTELLIGENT SYSTEMS YOU CAN TRUST, CONTROL AND EVOLVE.

TECHNOLOGY · PEOPLE · IDEAS · IMPACT

EU ARTIFICIAL INTELLIGENCE ACT

NexusOS AI Act Module

Functional Manual

How Cosmic Brokkoli records EU AI Act deployer duties in NexusOS — classification, registers, evidence, literacy and local AI.

CLASSIFY	RECORD	GOVERN	EVIDENCE
Record risk class and Art. 5 screening.	Living inventory of AI uses and duties.	Gaps, oversight, literacy and reminders.	Drive files, QMS documents and dossier export.

Cosmic Brokkoli UAB | Vilnius, Lithuania

AI ACT DOCUMENT

NexusOS AI Act Module — Functional Manual

Company	Cosmic Brokkoli UAB
Document type	AI Act Document — Functional / system manual
Classification	Internal
Document owner	AI Act / Compliance Coordinator (Marco Aveta)
Approval authority	CEO / Top Management (Stefania Aveta)
Version	20260901.01
Effective date	1 September 2026
Status	Approved / Controlled
Related document	NQMS v 20260831.01 — NexusOS QMS Functional Manual
Platform	NexusOS Business Suite — AI Act module

Contents

The table of contents below is a Word field. Open the document in Microsoft Word and use References → Update Table (update entire table) to populate page numbers after generation.

(Update this table of contents in Microsoft Word: References → Update Table.)

1. Purpose and scope

This controlled document describes the AI Act functions of NexusOS as implemented and operated by Cosmic Brokkoli UAB. It is written for a demanding compliance review: it explains what the system does, which data each register holds, and how that behaviour supports deployer duties under Regulation (EU) 2024/1689 (the EU Artificial Intelligence Act).

NexusOS is the organisational operating system in which Cosmic Brokkoli encodes its real workflows — projects, documented information, competence, suppliers and now AI inventory — rather than maintaining parallel spreadsheets. The AI Act module supports deployer accountability; it does not replace legal counsel, a notified body, or top-management decisions. NexusOS records your working classification — not a legal determination or conformity assessment.

- Scope of the software description: logon and identity, navigation into AI Act, every register (systems, duties, catalogues, literacy), the gap engine, dossier export, reminders, My tools for end users, and the on-premises AI Act agent (copilot).
- Out of scope: CE marking, Annex IV technical documentation, notified-body files, EU database filing, provider quality management systems, and detailed network or secrets configuration.
- Intended readers: compliance leads, DPOs, process owners, internal auditors, managers who maintain registers, and personnel who use assigned AI tools.

2. Regulatory background — EU AI Act (Regulation (EU) 2024/1689)

The EU Artificial Intelligence Act establishes harmonised rules for the development, placing on the market, putting into service and use of AI systems in the Union. Its objectives are to improve the functioning of the internal market, promote the uptake of human-centric and trustworthy AI, and protect health, safety, fundamental rights, democracy, the rule of law and the environment from harmful effects of AI, while supporting innovation.

The Act adopts a risk-based approach. Obligations depend on the role of the economic operator (provider, deployer, importer, distributor, authorised representative) and on the risk category of the AI system. NexusOS is designed primarily for deployers — organisations that use AI systems under their authority — and for internal inventory of SaaS tools and operational AI uses.

2.1 Economic operator roles

Role	Meaning and NexusOS coverage
Provider	Develops an AI system or has it developed and places it on the market or puts it into service under its own name or trademark. Provider obligations (Art. 16–17, Annex IV, conformity assessment) are outside this product.
Deployer	Uses an AI system under its authority except where the system is used in the course of a personal non-professional activity. Art. 26 sets deployer obligations NexusOS helps record.
Importer	Places on the market an AI system bearing the name or trademark of a person

	established outside the Union. Recorded as orgRole on a system where relevant.
Distributor	Makes an AI system available on the Union market without being provider or importer. Recorded as orgRole on a system where relevant.

When a user indicates that the organisation supplies an AI system to customers or other organisations, NexusOS sets a provider-fork flag. The product does not implement a provider QMS; the user shall seek specialist advice if placing AI on the market as a provider.

2.2 Risk pyramid and product mapping

The Act distinguishes four practical tiers for deployer inventory purposes:

Tier	Regulatory meaning / NexusOS behaviour
Prohibited AI (Art. 5)	Certain practices are banned (e.g. subliminal manipulation, untargeted scraping of facial images, social scoring by public authorities, emotion inference in workplace/education except medical/safety, biometric categorisation inferring sensitive attributes). NexusOS records Art. 5 screening checks — cleared or not — on each system; this is screening, not a legal clearance.
High-risk (Art. 6 + Annex III)	AI systems listed in Annex III (biometrics, critical infrastructure, education, employment, essential services, law enforcement, migration, justice, etc.) are high-risk when they pose significant risk to health, safety or fundamental rights. Deployers must meet Art. 26 obligations including use in accordance with instructions, human oversight, monitoring, logging, and — where applicable — FRIA (Art. 27).
Limited risk (Art. 50)	AI systems that interact directly with natural persons (e.g. chatbots) or generate synthetic audio, image, video or text shall meet transparency obligations. NexusOS maintains a transparency register per system.
Minimal risk	All other AI systems. The Act encourages voluntary codes of conduct; NexusOS still records them in the inventory for governance.

2.3 Key articles mapped to NexusOS

Article	Topic / NexusOS feature
Art. 4 — AI literacy	Providers and deployers shall take measures to ensure a sufficient level of AI literacy of their staff. Literacy courses and assignments register who passed what, with dates and scores.
Art. 5 — Prohibited practices	Classification wizard step 5 and system Art. 5 checks screen the seven prohibited-practice categories.
Art. 26 — Deployer obligations	Systems inventory: intended purpose, instructions, logging, oversight, monitoring, registration in EU database where required.
Art. 27 — FRIA	Fundamental Rights Impact Assessment register for high-risk deployers before

	putting into service.
Art. 50 — Transparency	Notices for chatbots, synthetic content, emotion recognition and deepfakes.
Art. 71–72 — Documentation and logs	Evidence tab links policies, DPAs, instructions; logging flag on system; dossier export for audit.
Art. 73 — Serious incidents	Incident register with authority notification tracking.
Art. 86 — Explanation of decisions	Register of requests to explain individual decisions supported by high-risk AI.

2.4 Classification logic in NexusOS

The classify wizard and API apply deterministic heuristics (not a conformity assessment). From the user's answers:

- HIGH risk class when the system supports or makes decisions about people and an Annex III area is selected.
- LIMITED risk when the system interacts with people (chat, generated content, emotion/deepfake) but is not high-risk.
- MINIMAL risk otherwise.
- FRIA required when high-risk and the use is not classified purely as a staff SaaS tool.
- Art. 5 prohibitedCleared is true only when all seven screening codes are explicitly cleared.

Annex III areas supported in the product: Biometrics, Critical infrastructure, Education and vocational training, Employment and workers management, Essential private and public services, Law enforcement, Migration and border, Administration of justice, and AI as safety component of regulated products.

2.5 Phased application

The AI Act applies in stages. Prohibited practices apply from early application dates; obligations for general-purpose AI models and high-risk systems follow later tranches depending on system type and Annex classification. Organisations shall verify current deadlines against the Official Journal text and national transposition guidance. NexusOS reminders are operational nudges — not legal deadline calculators.

2.6 Relationship to GDPR and ISO 9001

AI systems often process personal data. Where a DPIA is required under GDPR, NexusOS allows linking QMS controlled documents (from the Quality module) as DPIA evidence on the system Evidence tab. Drive files remain the storage layer; QMS document control and AI Act evidence metadata stay linked. This mirrors the ISO 9001 principle of controlled documented information (§7.5) applied alongside AI-specific registers.

3. The organisation — Cosmic Brokkoli

3.1 Mission and AI governance positioning

Cosmic Brokkoli UAB (company code 307504828, Vilnius, Lithuania) builds intelligent systems customers can trust, control and evolve. Public positioning states expertise across engineering, AI, data, hardware, design and governance — with privacy, security, GDPR and EU AI Act awareness treated as design constraints, not appendices.

For the AI Act module, that means: inventory and evidence must survive audit scrutiny; classification must be traceable to user answers; gaps must be visible before an incident or regulator question; and assistance from AI copilots must remain under human oversight with on-premises inference by default.

3.2 Why a living inventory beats spreadsheets

Deployer duties attach to specific AI systems in use — Copilot licences, HR scoring tools, chatbots, local Ollama deployments. Spreadsheets drift from reality within weeks. NexusOS ties each system to coded records (SYS-...), assigned users, linked suppliers and models, duty registers (FRIA, transparency, oversight), and a computed gap list. Reclassification updates the same record; activity feeds show who changed what.

3.3 Local intelligence architecture

Cosmic Brokkoli selects intelligence placement deliberately: frontier models where advanced reasoning adds value under governance; private/hybrid environments for sensitive workloads; edge AI on devices; and local AI on the organisation's infrastructure for privacy, control and continuity. The NexusOS AI Act agent uses local Ollama — AI inventory and register text are not sent to a public SaaS LLM by default. This supports Art. 26 human oversight expectations and GDPR data-minimisation for compliance records.

4. Access, tenants and navigation

Access to NexusOS, including the AI Act module, requires successful authentication. Unauthenticated users cannot read or mutate AI Act registers.



Sign in to access your files



Sign in as Marco
marco@cosmicbrokkoli.com



or

Email *

Password *



Figure 1 — NexusOS logon screen — email/password and SSO entry points

4.1 Session, company (tenant) and roles

After logon the user operates in one or more companies (tenants). All AI Act registers are tenant-scoped: codes, sequences and records do not leak across companies. Business roles constrain access:

Role	AI Act permissions
MEMBER	Read-only My tools — assigned IN_USE systems, literacy status, transparency notices, linked files.
MANAGER	Full register access: classify, systems, duties, catalogues, literacy, dossier, settings view.
ADMIN	May trigger the manual reminder check in AI Act settings.

From the authenticated shell, AI Act is reached under Business Suite. The sidebar lists: Overview, Classify, SaaS tools, AI systems, High-risk, Deployer duties, Literacy, Catalogues, Dossier, My tools, About, and Settings.

🔍 Search menu...

📄 Quotes

📅 Calendar

🕒 Time attendance

📅 Absences

☑️ Quality (QMS)

☑️ Overview

📄 Controlled documents

📊 Risks & opportunities

📋 Quality objectives



Business Suite > My Dashboard

My Dashboard

Hi Marco, today you have a few things to do

Day

8/31/2026

IN

Day - Monday, August 31, 2026

Presence status: IN

Figure 2 — Authenticated navigation — Business Suite and AI Act in the application shell

The company selector in the AI Act shell (AiActShell) binds every query to that tenant. Changing company changes visible registers and dossier content.

5. AI Act overview (landing)

The landing page (/business/ai-act) is the management dashboard for deployer duties. It offers start-here paths, open-gap KPIs, literacy coverage percentage, and links to dossier export and product scope (About).

Business Suite > AI Act for this company

AI Act for this company Company: Cosmic Brokkoli (CB)

Start from how you use AI. Registers stay available when you need them.

⚠ At least one system is flagged as possibly placing you in a provider role. This product does not implement a provider QMS.

Start here

Classify a use
Answer a short questionnaire. We record the risk class and which duties apply.
[Start classification](#)

Register a SaaS tool
Copilot, ChatGPT and similar staff tools — without forcing FRIA.
[Open SaaS tools](#)

Open inventory
All AI systems, including high-risk and operational uses.
[View systems](#)

Open gaps
What is still missing for deployer duties on systems in this company.

4 blockers 12 warnings Literacy coverage 43%

🔍 Search gaps...

System	Name	Gap	Severity
AIS-2026-0001	Microsoft 365 Copilot	User without current literacy	Warning
AIS-2026-0001	Microsoft 365 Copilot	User without current literacy	Warning
AIS-2026-0001	Microsoft 365 Copilot	User without current literacy	Warning
AIS-2026-0001	Microsoft 365 Copilot	User without current literacy	Warning
AIS-2026-0001	Microsoft 365 Copilot	User without current literacy	Warning

AI Act agent

Figure 3 — AI Act overview — start-here paths, gap counts and literacy coverage

- Classify a use — short questionnaire creating/updating a draft system with derived risk class.

- Register a SaaS tool — Copilot, ChatGPT and similar staff tools without forcing FRIA.
- Open inventory — all AI systems including high-risk and operational uses.

Open gaps are computed from active (non-retired) systems. Severities: Blocker (must fix before credible compliance posture), Warning (should fix), Info (advisory). A provider-fork banner appears when at least one system is flagged as possibly placing the organisation in a provider role.

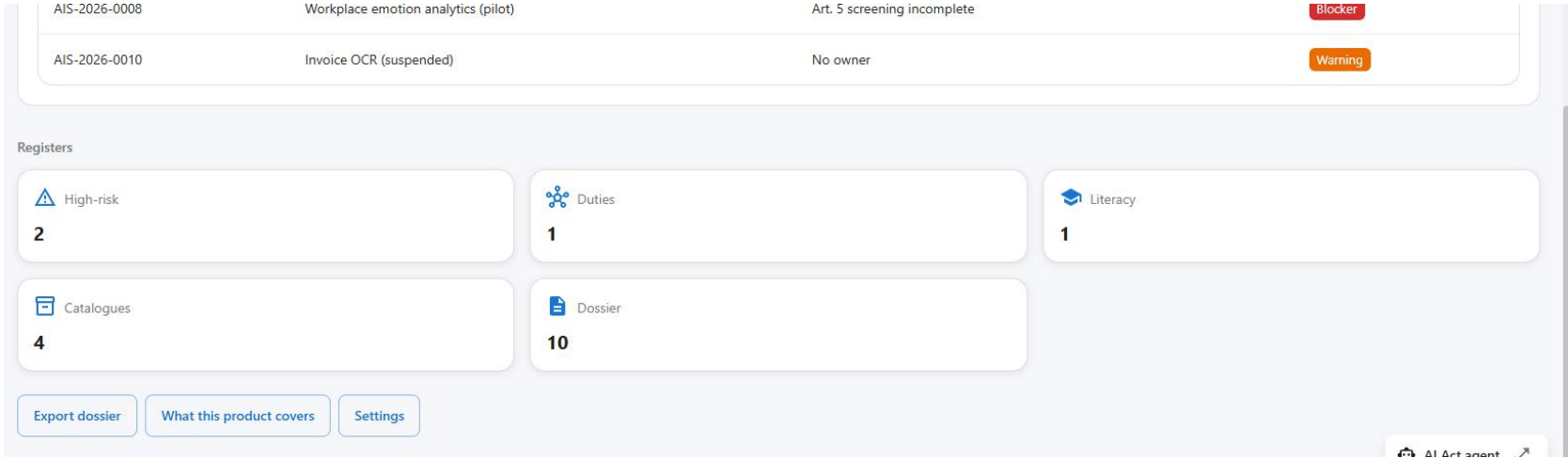


Figure 4 — Register hub cards — quick navigation to duty and catalogue areas

Overview element	Meaning
blockers / warnings counts	Aggregated gap severities across the tenant.
literacyCoverage percent	Share of assigned system users with current passed literacy.
registers cards	Links to duties, catalogues and other areas.
export dossier	Jump to printable / Excel audit inventory.

6. Classification wizard

The classify flow (/business/ai-act/classify) is the recommended entry point for new AI uses. It is explicitly not a conformity assessment — it records a draft system from structured answers.

Business Suite > AI Act > **Classify an AI use**

Classify an AI use

Not a conformity assessment. Records a draft system from your answers.

Company
Cosmic Brokkoli (CB) ▼

Info Add one use of AI here. The inventory lives under Systems and SaaS tools.

Microsoft 365 Copilot ChatGPT Team CV ranking (employment)

1 2 3 4 5

What is it Do we sell it How we use it People and data Art. 5 screening

Likely class from your answers
Minimal — FRIA: no
This is not a conformity assessment.

Name *

Intended purpose

Department

Back Next

Figure 5 — Classify wizard — identity, role fork, use kind, people and data, Art. 5 screening

6.1 Wizard steps

Step	Content
Step 1 — Identity	Name, intended purpose, department; optional supplier and owner.
Step 2 — Role fork	Whether the organisation supplies the system to third parties (provider fork warning).
Step 3 — Use kind	SAAS_TOOL (staff tools), OPERATIONAL (HR, scoring, public services), or OTHER.
Step 4 — People and data	Interacts with people; decisions about people; Annex III area; personal data and categories.
Step 5 — Art. 5 screening	Seven prohibited-practice checkboxes — each must be cleared to pass screening.

6.2 Presets and live preview

Presets accelerate common entries: Microsoft Copilot, ChatGPT, Gemini, Claude, Ollama, CV ranking and similar. The live preview shows the likely risk class and whether FRIA is required before submit. Submit calls POST /api/v1/business/ai-act/classify and redirects to system detail. Reclassify opens the wizard with ?systemId= pre-filled.

Answer combination	Derived outcome
decisionsAboutPeople + annexIiArea	Derives HIGH risk class and stores Annex III label.
interactsWithPeople (not high)	Derives LIMITED risk class.
Otherwise	MINIMAL risk class.
High-risk and not SAAS_TOOL only	friaRequired = true.
art5Checks all cleared	prohibitedCleared = true; else gap art5_not_cleared (blocker).

7. SaaS tools register

Staff SaaS tools (/business/ai-act/tools) are systems filtered to useKind = SAAS_TOOL. Typical examples: Microsoft Copilot, ChatGPT Enterprise, Google Gemini for Workspace. The register focuses on literacy, DPA availability via supplier, transparency where LIMITED risk, and user assignment — without forcing FRIA for pure staff-tool uses that are not high-risk.

Business Suite > AI Act > My AI tools

My AI tools

Tools this company assigned to you. Literacy status and transparency notices, read-only.

Company
Cosmic Brokkoli (CB)

Search tools...

Name	Code	Use kind	Status	Risk class	Passed	Linked files
Recruity CV ranking	AIS-2026-0003	Operational use	In use	High-risk	Literacy missing or expired	test.docx PDF_TestPage.pdf
ChatGPT Team	AIS-2026-0002	SaaS tool	In use	Limited (transparency)	Literacy missing or expired	AI Smart Garage OS.pdf
Microsoft 365 Copilot	AIS-2026-0001	SaaS tool	In use	Limited (transparency)	Literacy missing or expired	NexusOS.pptx ITR FULL PROJECT.pdf Why_Nexus.pdf

Figure 6 — SaaS tools register — staff AI tools filtered from the systems inventory

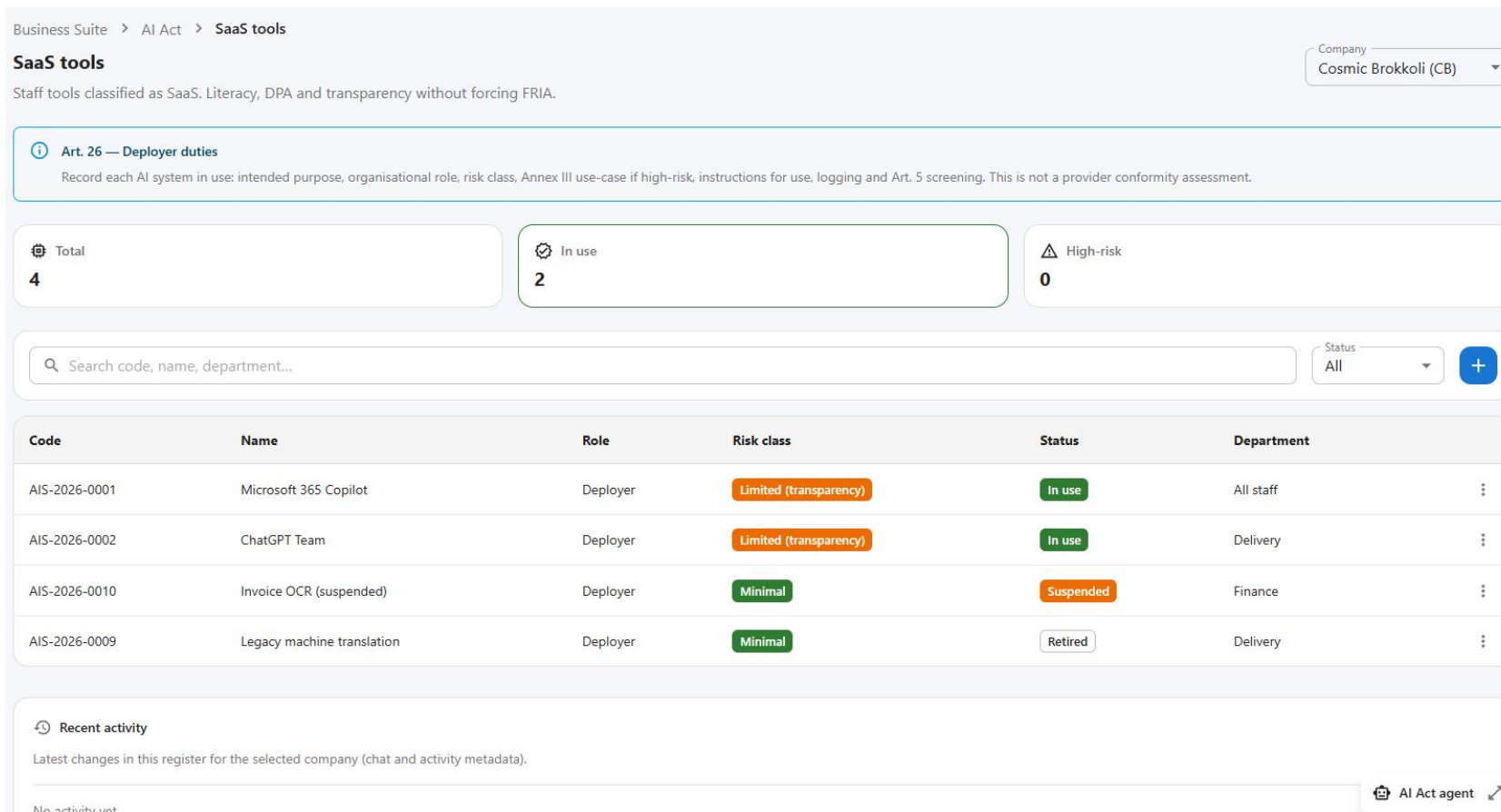


Figure 7 — SaaS tool detail — presets, risk class and deployer metadata

Field	SaaS tool behaviour
useKind	SAAS_TOOL — distinguishes staff tools from operational systems.
riskClass	Often MINIMAL or LIMITED; HIGH if decisions-about-people in Annex III area.
supplier / model	Links to catalogue registers for DPA and infrastructure tracking.
status	DRAFT → IN_USE when actively deployed to staff.

8. AI systems inventory

The full inventory (/business/ai-act/systems) lists every AI system the organisation deploys, imports or distributes: operational HR tools, public-facing chatbots, internal analytics, and SaaS tools. Summary KPIs show total, in use, and high-risk counts.

Business Suite > AI Act > AI systems > AIS-2026-0001 — Microsoft 365 Copilot

AIS-2026-0001 — Microsoft 365 Copilot

Limited (transparency)

Limited (transparency)

In use

Intended purpose

Draft emails, summarise meetings and assist with internal documents.

SaaS tool

Not subliminal or manipulative techniques

Does not exploit vulnerabilities

Not social scoring

Not untargeted predictive policing

Not untargeted facial-image scraping

Not emotion recognition at work or school (prohibited cases)

Not prohibited biometric categorisation

Reclassify

Copy staff instructions

GapsEvidenceUsersRelated registers

Search gaps...

Gap	Severity
User without current literacy	Warning
User without current literacy	Warning
User without current literacy	Warning
User without current literacy	Warning
User without current literacy	Warning

AI Act agent

Figure 8 — AI systems register — code, role, risk class, status, Annex III, FRIA flag

Business Suite
> AI Act
> AI systems
> AIS-2026-0001 — Microsoft 365 Copilot

AIS-2026-0001 — Microsoft 365 Copilot

Company
Cosmic Brokkoli (CB)

Limited (transparency)

Limited (transparency)

In use

Intended purpose
Draft emails, summarise meetings and assist with internal documents.

SaaS tool

Not subliminal or manipulative techniques

Does not exploit vulnerabilities

Not social scoring

Not untargeted predictive policing

Not untargeted facial-image scraping

Not emotion recognition at work or school (prohibited cases)

Not prohibited biometric categorisation

Reclassify

Copy staff instructions

Gaps

Evidence

Users

Related registers

Search...

Evidence type	File
DPA	NexusOS.pptx
Instructions for use	ITR FULL PROJECT.pdf
Policy	Why_Nexus.pdf

Figure 9 — System create/edit dialog — purpose, logging, instructions, EU DB registration

Field	Regulatory / system meaning
code	SYS-... assigned per tenant by numbering service.
orgRole	DEPLOYER, IMPORTER, or DISTRIBUTOR.
intendedPurpose	Art. 26 — use in accordance with instructions requires a clear purpose statement.
riskClass	PROHIBITED_SCREEN, HIGH, LIMITED, MINIMAL — from classification.
annexliiArea	Required label when high-risk.
status	DRAFT, IN_USE, SUSPENDED, RETIRED.
loggingEnabled	Whether automatic logging of events is enabled (Art. 26(8)).
instructionsReceived	Whether deployer received provider instructions for use.
euDbRegistration	Reference if registered in EU database where applicable.
ownerUserId	Accountable owner — missing owner triggers gap.
friaRequired	Flag from classification; drives FRIA gap when no completed FRIA.

9. High-risk systems

The high-risk view (/business/ai-act/high-risk) filters systems where riskClass = HIGH. The UI displays Art. 26 deployer duty hints. High-risk deployers shall use the system according to instructions, ensure human oversight, monitor operation, keep logs, and complete FRIA where required before putting into service.

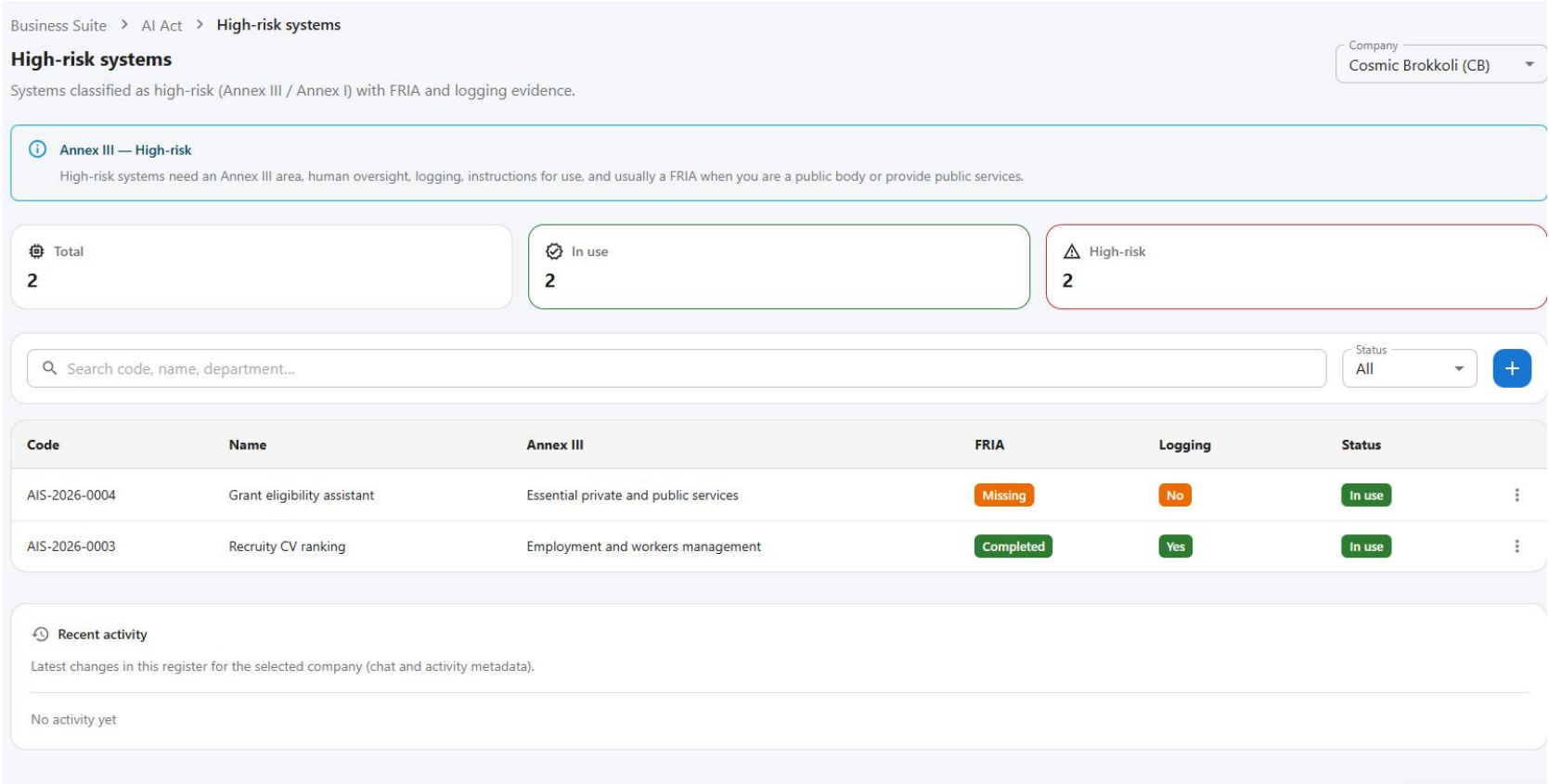


Figure 10 — High-risk systems list — Annex III areas and FRIA status

Business Suite > AI Act > AI systems > AIS-2026-0004 — Grant eligibility assistant

AIS-2026-0004 — Grant eligibility assistant

High-risk

High-risk In use

Intended purpose
Suggest whether an application meets published grant criteria.

Operational use · Essential private and public services · yes

Not subliminal or manipulative techniques Does not exploit vulnerabilities Not social scoring Not untargeted predictive policing Not untargeted facial-image scraping

Not emotion recognition at work or school (prohibited cases) Not prohibited biometric categorisation

Reclassify Copy staff instructions

Gaps Evidence Users Related registers

Search gaps...

Gap	Severity
Art. 5 screening incomplete	Blocker
FRIA not completed	Blocker
No human oversight	Blocker
Logging not enabled	Warning
Instructions not recorded	Warning

AI Act agent

Figure 11 — High-risk system — logging, instructions and oversight indicators

- Blocker gaps typical on high-risk: incomplete Art. 5, missing Annex III, missing completed FRIA, missing oversight.
- Warning gaps: logging disabled, instructions not confirmed, literacy gaps on assigned users.
- Each row links to system detail for gap closure.

10. System detail — gaps, evidence, users, related

System detail (/business/ai-act/systems/[id]) is the operational centre for one AI use. Four tabs structure deployer evidence and duties.

10.1 Gaps tab

The gap engine (AiActSmeService) evaluates each non-retired system and produces actionable items:

Gap code	Severity / meaning
provider_fork	Info — organisation may be acting as provider; seek specialist advice.
missing_owner	Warning — assign an accountable owner.
art5_not_cleared	Blocker — complete Art. 5 screening via reclassify.
missing_annex_iii	Blocker — high-risk system without Annex III area.
missing_fria	Blocker — FRIA required but no FRIA with outcome COMPLETED.
missing_oversight	Blocker — no human oversight record (Art. 26).
missing_logging	Warning — logging not enabled on high-risk system.
missing_instructions	Warning — instructions not marked received.
missing_transparency	Warning — LIMITED risk system without transparency notice (Art. 50).
missing_dpa	Warning — personal data use but supplier DPA not available.
missing_instructions_evidence	Info — instructions marked received but no INSTRUCTIONS evidence file linked.
literacy_gap	Warning — assigned user without current passed literacy (Art. 4).

Clicking a gap navigates to the register or tab where the user can close it (gapActions.ts).

10.2 Evidence tab

Evidence links Drive files or QMS controlled documents to the system. Supported kinds include POLICY, INSTRUCTIONS, DPA, ACCEPTABLE_USE, FRIA_DOC, DPIA (via QMS node), and OTHER. This implements the documentation expectation of Art. 71–72 at deployer level — evidence stays in Drive/QMS; NexusOS holds metadata and audit links.

10.3 Users tab

Assign employees who use the system. For each user the UI shows literacy covered or missing based on employee_literacy records (passed and non-expired end date). Literacy gaps on assigned users appear both here and on the overview.

10.4 Related tab

Deep links to FRIA, transparency, incidents, oversight and explanation records for this system. Actions include Reclassify and Copy staff instructions (template from aiAct.templates.instructionsStaff).

11. Deployer duties hub

The duties hub (/business/ai-act/duties) card-navigates to the five duty registers mandated for deployers under the Act's operational articles.

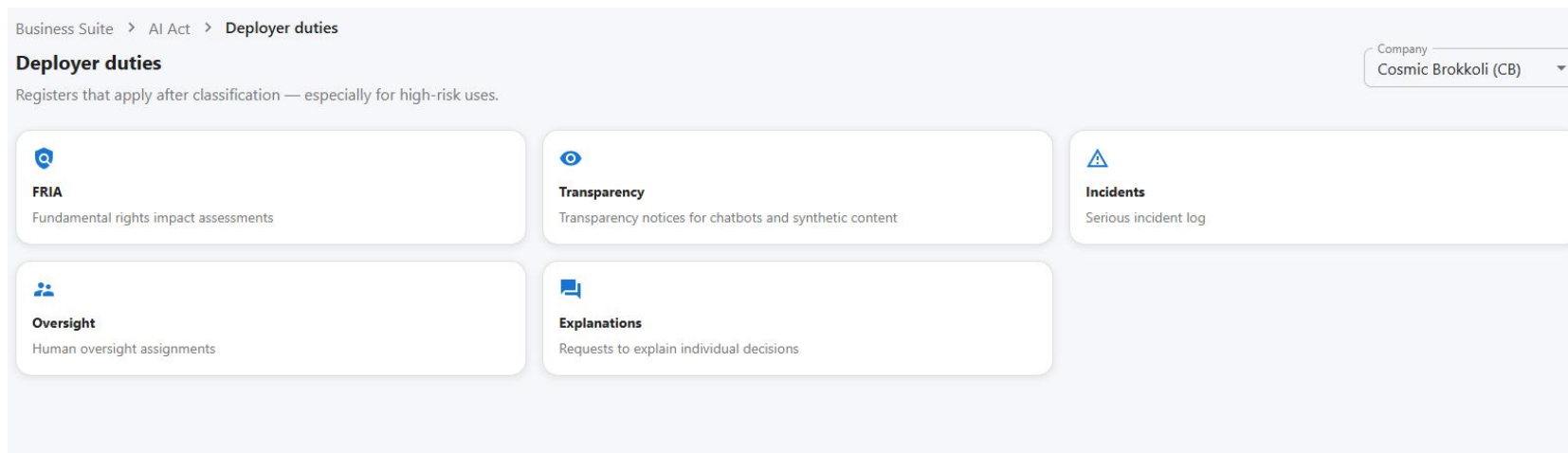


Figure 12 — Deployer duties hub — FRIA, transparency, incidents, oversight, explanations

12. FRIA — Fundamental Rights Impact Assessment (Art. 27)

Before putting a high-risk AI system into service, deployers shall perform a FRIA — except where the system is used for certain narrow purposes or an equivalent assessment exists. NexusOS maintains a register of FRIA records linked to systems.

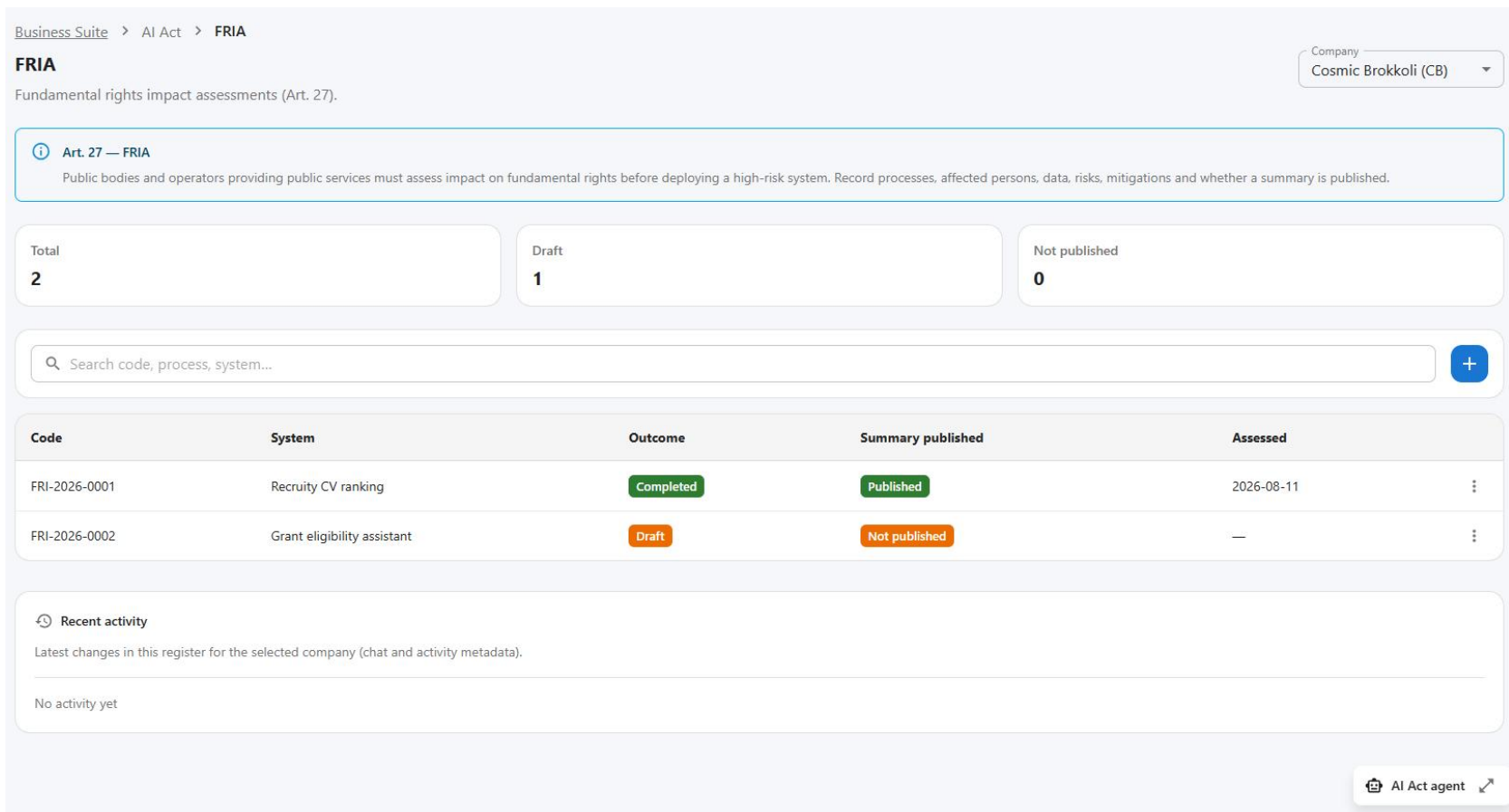


Figure 13 — FRIA register — processes, persons affected, outcome and reviewer

Field	FRIA content
code	FRIA-... per tenant.
systemId	Linked high-risk AI system.
processesDescription	Processes where the system is used.
personsAffected	Categories of persons affected.
dataUsed	Data categories processed.
risks / mitigations	Fundamental rights risks and mitigation measures.
oversightMeasures	Human oversight measures applied.
outcome	DRAFT, COMPLETED, NOT_REQUIRED — only COMPLETED closes missing_fria gap.
assessmentDate / reviewDate	When assessed; review date drives reminder notifications.
summaryPublished	Whether a summary was published per Art. 27(7).

reviewerUserId	Person who reviewed the assessment.
----------------	-------------------------------------

13. Transparency (Art. 50)

Deployers of AI systems that interact directly with natural persons, or that generate synthetic content, shall ensure transparency — informing users they are interacting with AI or that content is artificially generated. NexusOS records notices per system.

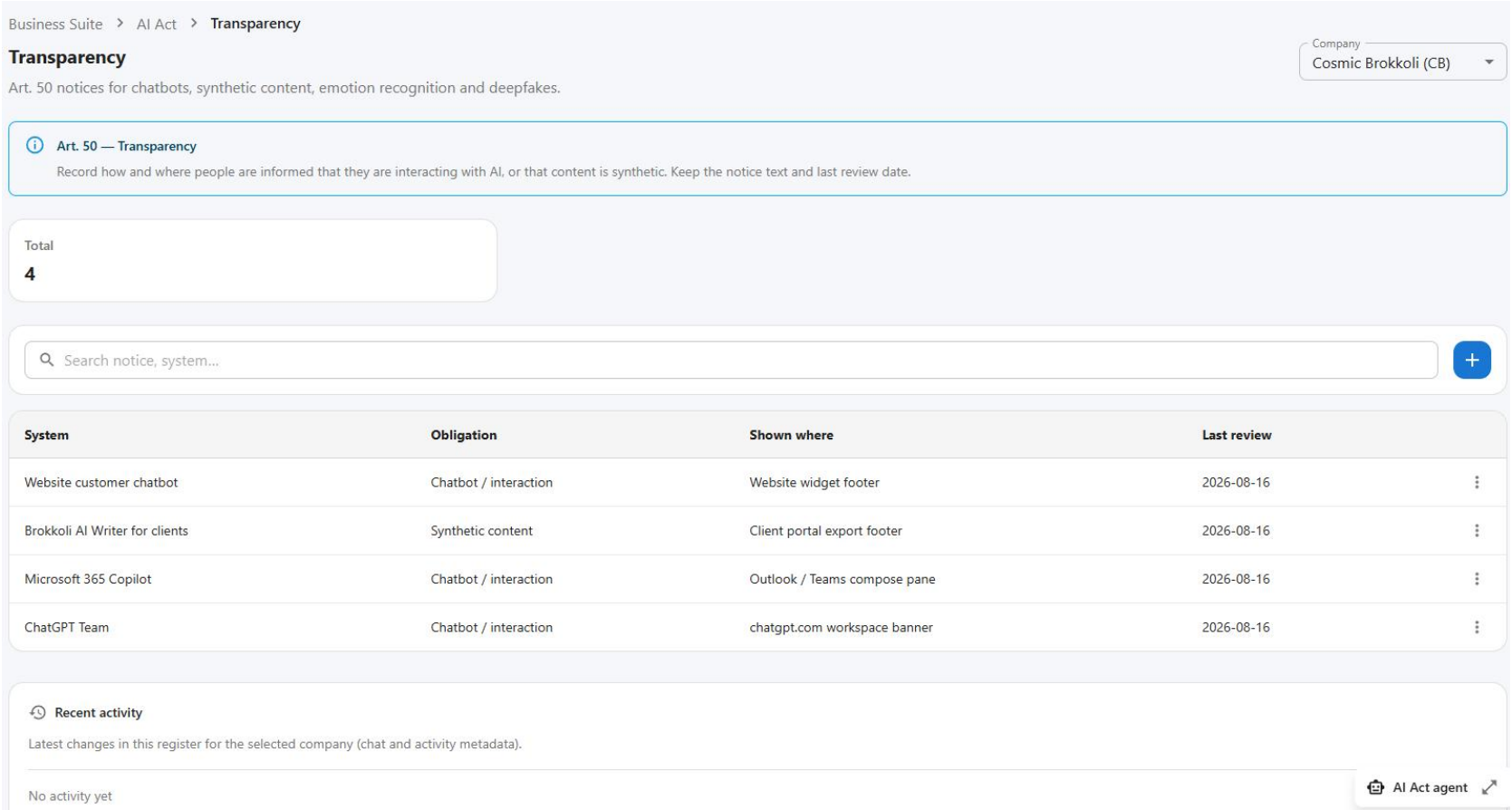


Figure 14 — Transparency register — obligation type, notice text, where shown

Field	Transparency record
obligationType	CHATBOT, SYNTHETIC_CONTENT, EMOTION, DEEPFAKE — maps to Art. 50 paragraphs.

noticeText	The disclosure shown to users.
whereShown	UI location, email footer, watermark, etc.
lastReviewDate	When the notice was last reviewed.

Template insert buttons help draft standard chatbot and synthetic-content notices.

14. Serious incidents (Art. 73)

Deployers of high-risk AI systems shall report serious incidents to the provider and, where applicable, to market surveillance authorities without undue delay. NexusOS logs incidents with severity and notification tracking — it does not file reports to authorities automatically.

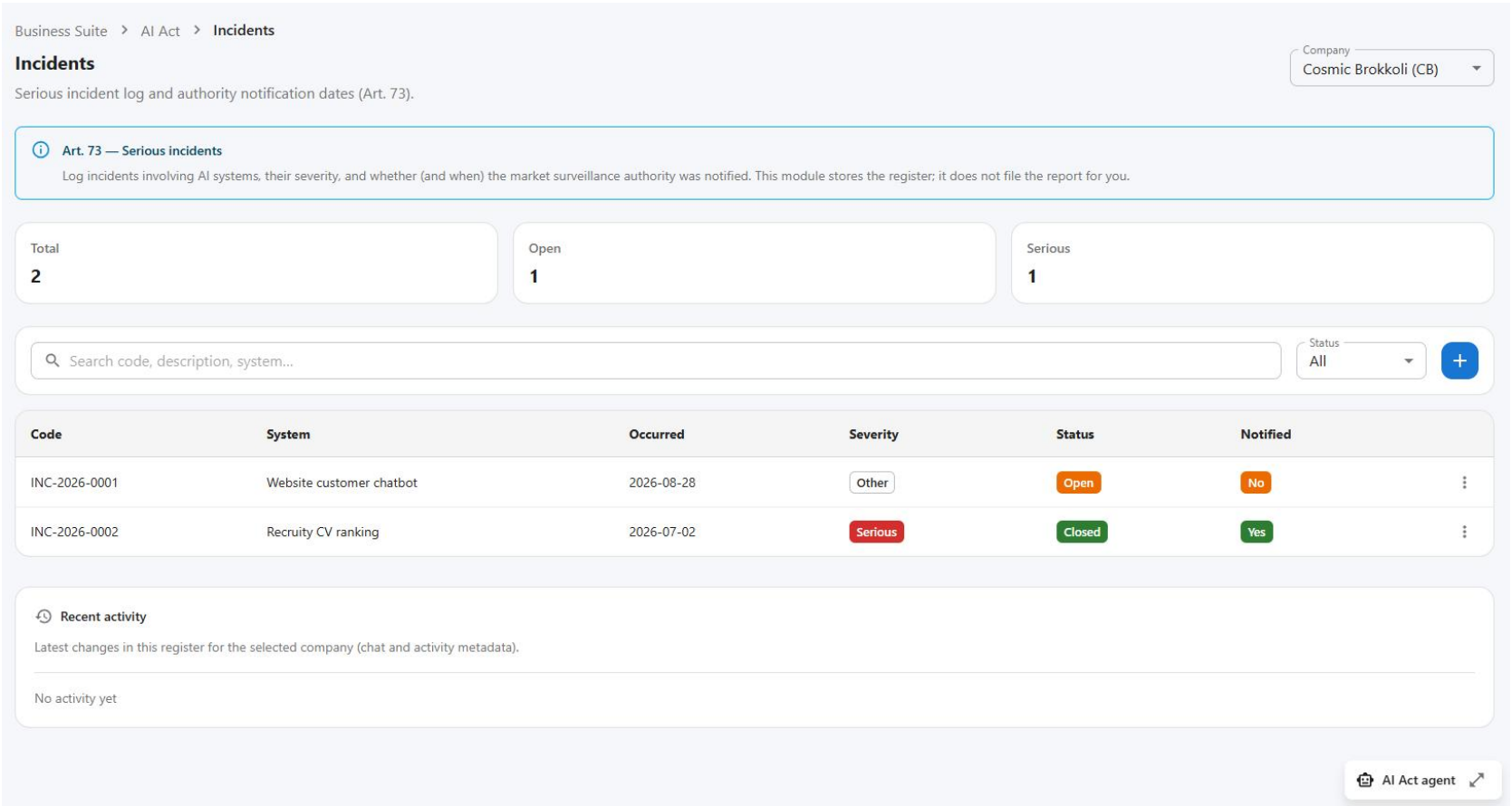


Figure 15 — Incidents register — severity, notification status and authority

Field	Incident record
code	INC-... per tenant.
occurredAt	When the incident occurred.
severity	SERIOUS or OTHER.
description	What happened.
notified	Whether authority/provider notification was made.
notificationDate / authority	When and to whom notified.
status	OPEN, NOTIFIED, CLOSED.

15. Human oversight (Art. 26)

High-risk AI systems shall be designed and used so that natural persons effectively oversee them. Deployers assign oversight to competent persons with authority to override decisions where appropriate.

Business Suite
> AI Act
> Human oversight

Company
Cosmic Brokkoli (CB)

Human oversight

People assigned to oversee AI systems, with override rights and training dates.

i
Art. 26 — Human oversight

Assign named people who can monitor the system, understand its output and override or interrupt it. Record instructions and training dates.

Total
2

Can override
2

+

System	Person	Role	Can override	Trained	
Recruity CV ranking	Maurizio Civerchia	HR lead — human reviewer	Yes	2026-07-12	⋮
Recruity CV ranking	Marco Aveta	Deputy reviewer	Yes	2026-07-12	⋮

🕒
Recent activity

Latest changes in this register for the selected company (chat and activity metadata).

No activity yet

AI Act agent

Figure 16 — Human oversight register — person, role, override rights, training

Field	Oversight record
userId	Employee assigned oversight responsibility.
roleDescription	Role in the oversight process.
instructions	How to monitor and intervene.
canOverride	Whether the person can override system output.
trainingDate	When oversight training was completed.

16. Explanation of decisions (Art. 86)

Affected persons may request an explanation of a decision taken by a high-risk AI system that affects them in a legal or similarly significant way. NexusOS tracks requests and responses.

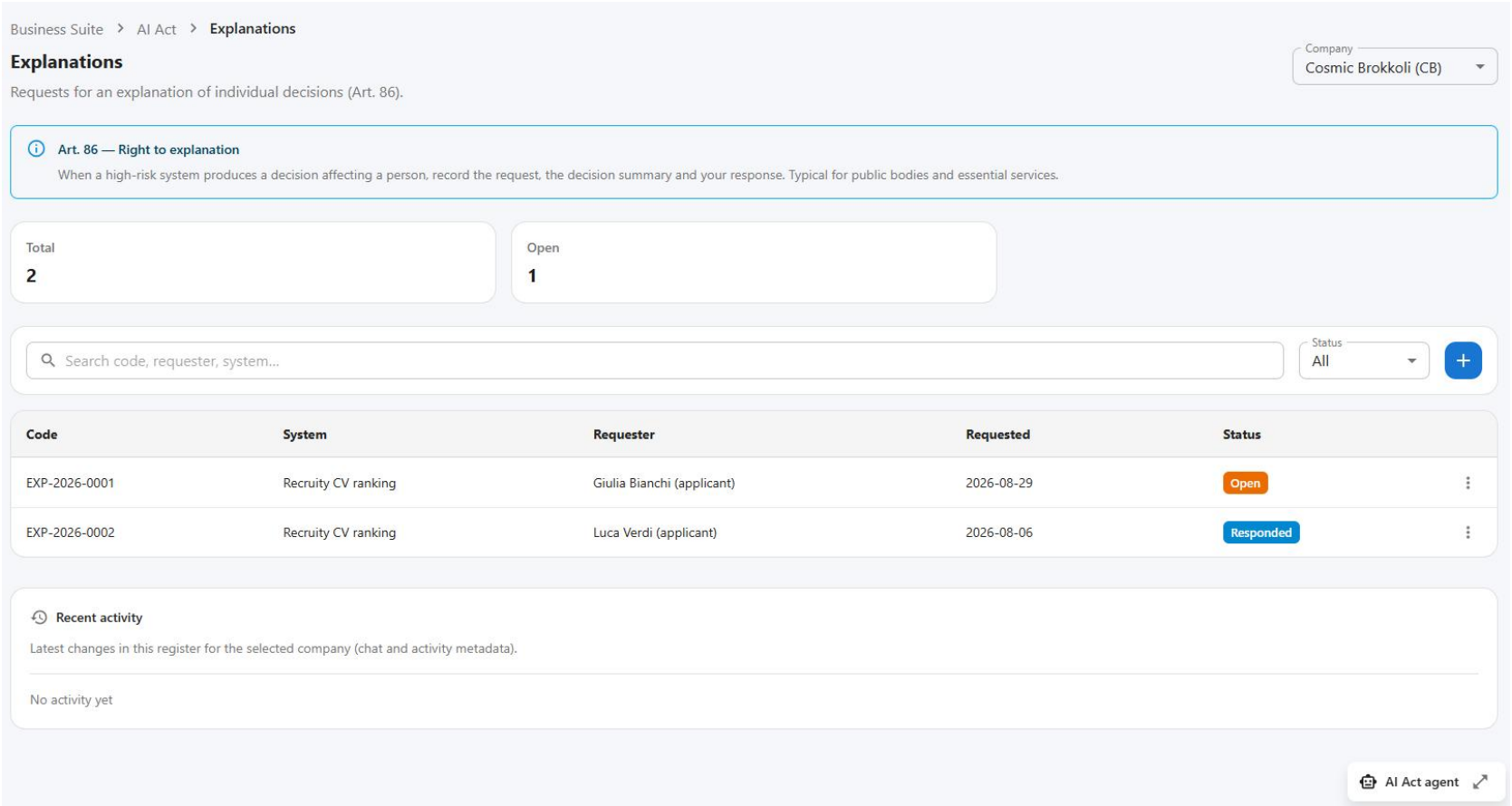


Figure 17 — Explanations register — requester, decision summary, response status

Field	Explanation record
code	EXP-... per tenant.
requester	Person who requested explanation.
requestedAt	Date of request.
decisionSummary	Decision the explanation relates to.
response	Explanation provided.

status	OPEN, RESPONDED, CLOSED.
--------	--------------------------

17. Catalogues hub

Supporting registers (/business/ai-act/catalogues) maintain suppliers, models, course providers and literacy courses. Typical setup order: providers → courses → suppliers → models.

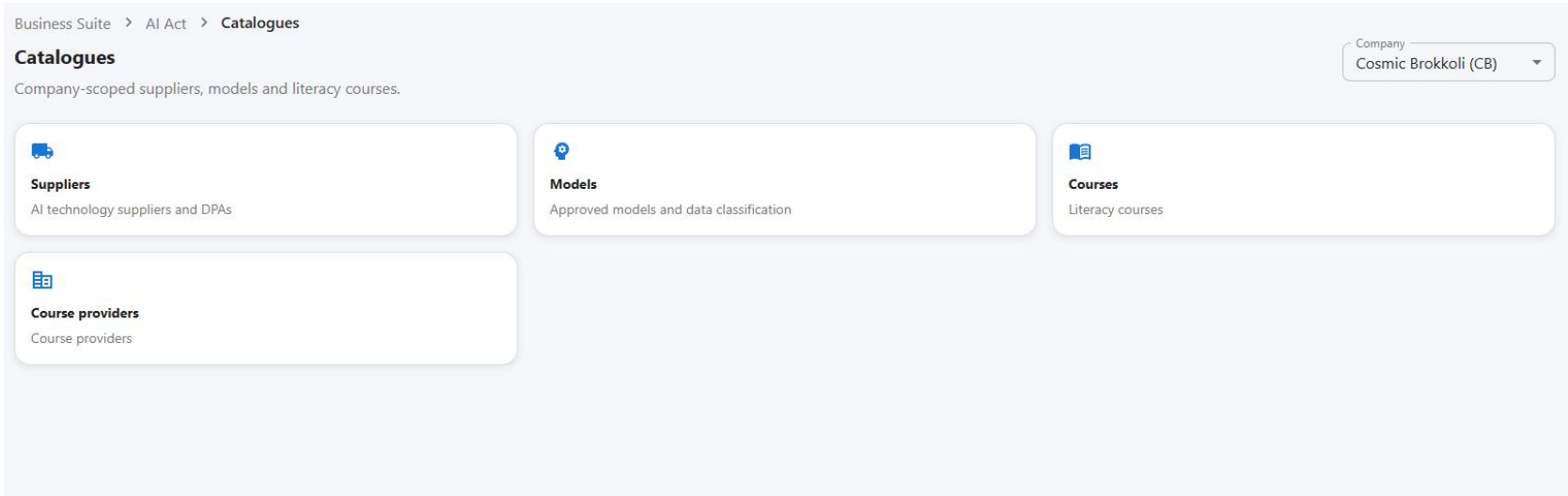


Figure 18 — Catalogues hub — suppliers, models, courses, providers

18. AI suppliers

AI technology suppliers (cloud AI vendors, SaaS providers, integrators) are recorded with contact data, approval status, risk level, and DPA availability. Suppliers without DPA where personal data is used trigger missing_dpa gaps on linked systems.

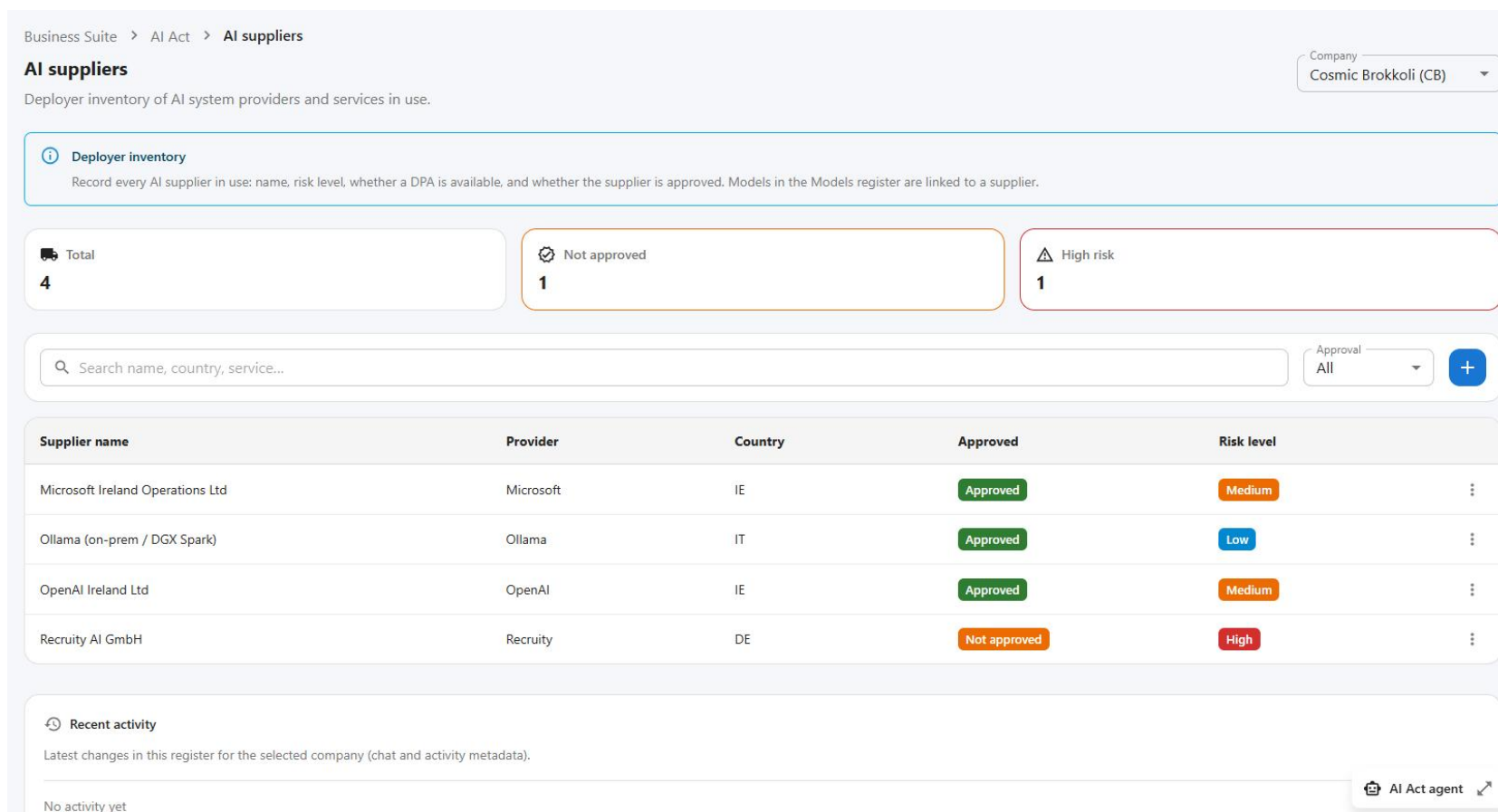


Figure 19 — AI suppliers register — DPA, approval, risk level, last review

Field	Supplier record
name / contacts / website	Supplier identity.
riskLevel	LOW through REALLY_HIGH — organisational risk assessment.
dpaAvailable	Whether a data processing agreement exists.
approvalStatus	PENDING, APPROVED, REJECTED.
lastReviewDate	Drives supplier review reminders (>12 months).

19. AI models

Models catalogue tracks LOCAL vs CLOUD infrastructure, data classification (PUBLIC through SPECIAL_CATEGORY_DATA), version, and supplier link. Systems reference a model for traceability from use case to underlying model and hosting.

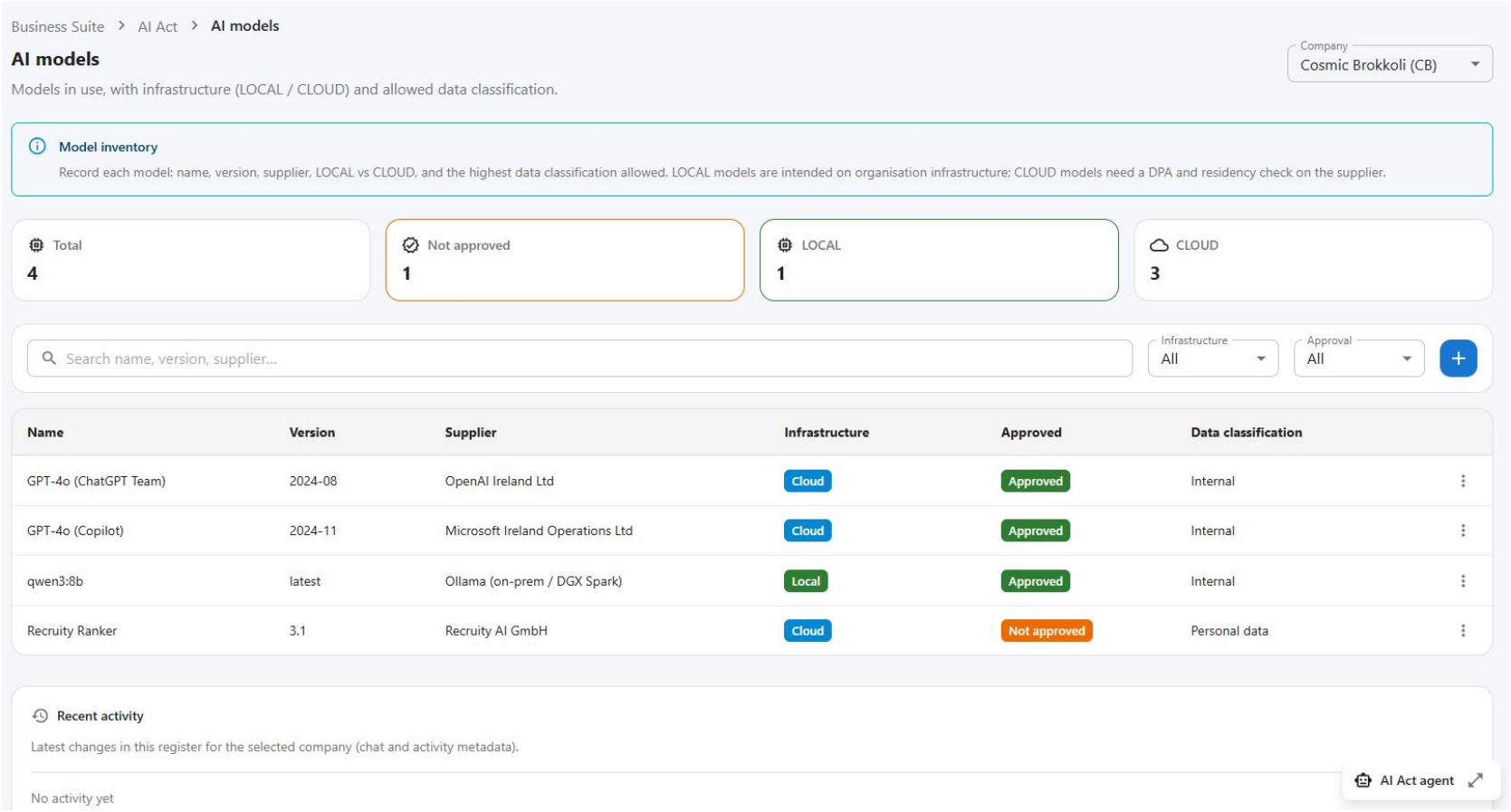


Figure 20 — AI models register — LOCAL/CLOUD, data classification, approval

20. Course providers and literacy courses

Course providers are legal entities delivering AI literacy training. Courses link to a provider and form the catalogue from which literacy assignments are made.

Business Suite > AI Act > Course providers

Course providers

Providers of AI literacy courses used for Art. 4 training.

Company
Cosmic Brokkoli (CB)

Art. 4 — AI literacy

Keep an inventory of organisations that deliver AI literacy training. Courses in this module are linked to a provider so assignments to people stay traceable.

Total

2

With courses

2

Search name, legal name, country...

+

Name	Legal name	Country	Tax ID	Website	
EU AI Literacy Institute	EU AI Literacy Institute ASBL	BE	BE0123456789	https://example.invalid/literacy	⋮
Internal HR Academy	Cosmic Brokkoli HR Academy	IT	IT00000000000	—	⋮

Recent activity

Latest changes in this register for the selected company (chat and activity metadata).

No activity yet

AI Act agent

Figure 21 — Course providers register — legal entity information

Business Suite > AI Act > AI literacy courses

AI literacy courses

Company
Cosmic Brokkoli (CB)

Catalogue of AI literacy courses assigned to people.

Art. 4 — AI literacy courses
Record the courses used to build AI literacy. Each course is tied to a provider. Assignments (who took which course, and whether they passed) are in the Literacy register.

Total
2

Search name or provider...

Name	Provider	Description
AI literacy for staff (Art. 4)	EU AI Literacy Institute	Four-hour course: what is an AI system, prohibited practices, when to escalate, acceptable use of Copilot/ChatGPT.
High-risk deployer duties (employment)	Internal HR Academy	FRIA, human oversight, logging and contestability for employment-related AI.

Recent activity

Latest changes in this register for the selected company (chat and activity metadata).

No activity yet

AI Act agent

Figure 22 — Literacy courses catalogue — linked to providers

21. Literacy assignments (Art. 4)

AI literacy assignments record which employee completed which course, with start/end dates, test score, and passed/not passed. The same data is editable from Employees → Literacy tab. Current literacy requires passed = true and end_date not expired.

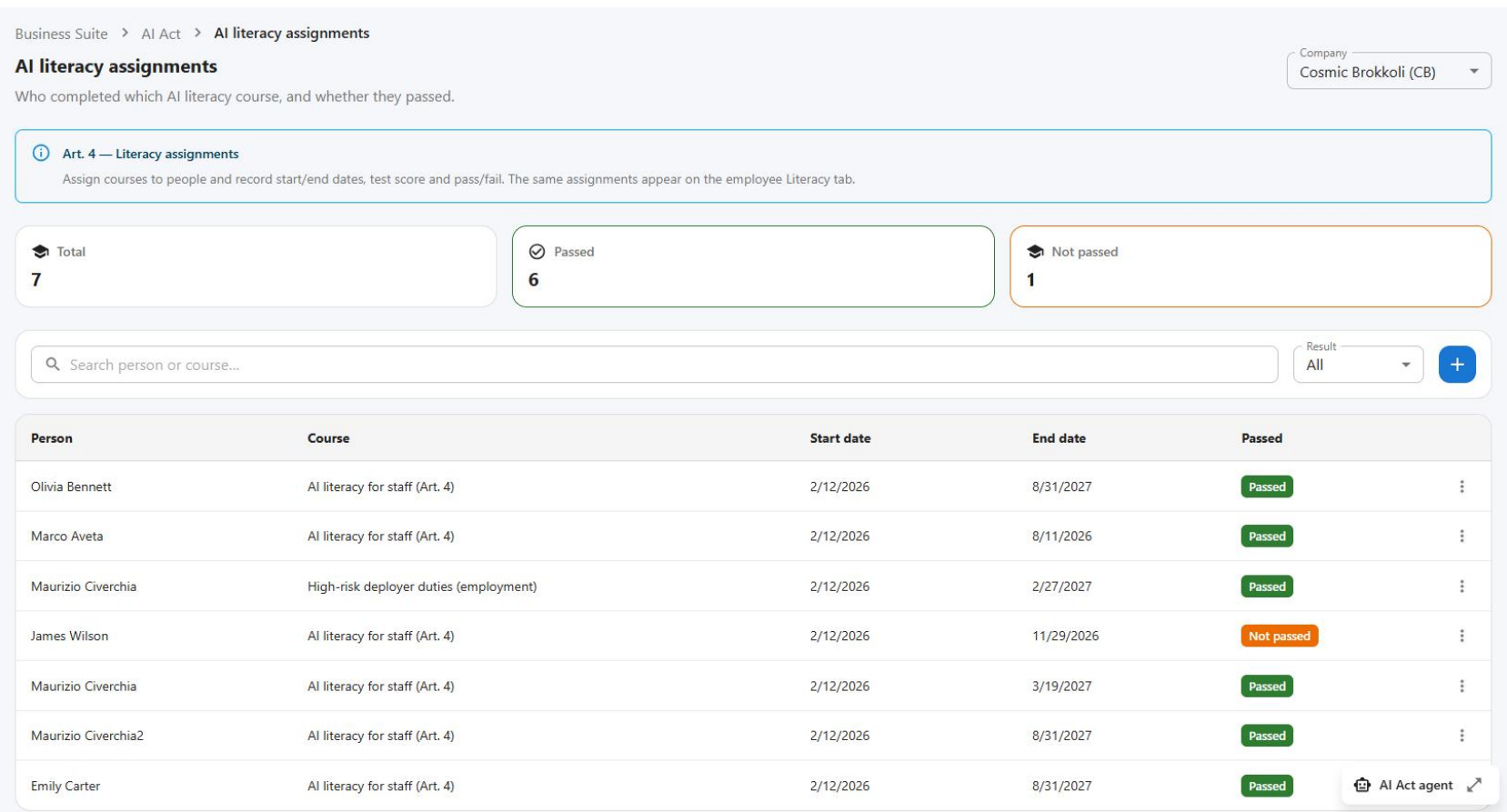


Figure 23 — Literacy assignments — employee, course, dates, pass status

Edit assignment

Person *

Olivia Bennett

Course *

AI literacy for staff (Art. 4)

Start date *

02/12/2026

End date

08/31/2027

Test score

80

☒ Passed

Notes

Completed classroom + quiz.

Record activity

History of create, update, treatment actions and notes for this item.

No activity yet

Actions on this entity will appear here

Cancel

Save

Figure 24 — Literacy assignment detail — scores and validity period

Field	Literacy assignment
employeeId	Person who took or will take the course.
courseId	Catalogue course (Art. 4 literacy measure).
startDate / endDate	Validity window; expired end_date fails literacy check.
testScore / passed	Outcome evidence.

22. Dossier export

The dossier (/business/ai-act/dossier) produces a printable inventory for internal audit. The subtitle states explicitly: not a notified-body file. API: GET /api/v1/business/ai-act/dossier?tenantId=...

Business Suite > AI Act > AI Act dossier

AI Act dossier

Company
Cosmic Brokkoli (CB)

Print / PDF
Download Excel

Printable inventory for internal audit. Not a notified-body file.

Systems in use

Search this section...

Code	Name	Risk class	Use kind	Status	Owner	Supplier
AIS-2026-0001	Microsoft 365 Copilot	LIMITED	SAAS_TOOL	IN_USE	Maurizio Civerchia	Microsoft Ireland Operations Ltd
AIS-2026-0002	ChatGPT Team	LIMITED	SAAS_TOOL	IN_USE	Marco Aveta	OpenAI Ireland Ltd
AIS-2026-0003	Recruity CV ranking	HIGH	OPERATIONAL	IN_USE	Maurizio Civerchia	Recruity AI GmbH
AIS-2026-0004	Grant eligibility assistant	HIGH	OPERATIONAL	IN_USE	Maurizio Civerchia	OpenAI Ireland Ltd
AIS-2026-0005	Website customer chatbot	LIMITED	OPERATIONAL	IN_USE	Marco Aveta	OpenAI Ireland Ltd
AIS-2026-0006	Ollama QMS assistant	MINIMAL	OTHER	IN_USE	Maurizio Civerchia	Ollama (on-prem / DGX Spark)
AIS-2026-0007	Brokkoli AI Writer for clients	LIMITED	OPERATIONAL	IN_USE	Maurizio Civerchia	Ollama (on-prem / DGX Spark)
AIS-2026-0008	Workplace emotion analytics (pilot)	PROHIBITED_SCREEN	OPERATIONAL	DRAFT	Maurizio Civerchia	—
AIS-2026-0009	Legacy machine translation	MINIMAL	SAAS_TOOL	RETIRED	Marco Aveta	OpenAI Ireland Ltd
AIS-2026-0010	Invoice OCR (suspended)	MINIMAL	SAAS_TOOL	SUSPENDED	—	—

Open gaps

Search
AI Act agent

Figure 25 — Dossier — searchable tables and export actions

Sections included in the dossier and Excel export (aiact-dossier.xlsx):

- Systems in use
- Open gaps
- Literacy assignments
- FRIA records
- Incidents
- Suppliers

Print/PDF uses browser window.print() on printable sheets (.aiact-print-sheet). Excel export uses ?format=xlsx with six worksheets matching the sections above.

23. My tools (end users)

My tools (/business/ai-act/my-tools) is the read-only end-user view (MEMBER role). It lists IN_USE systems assigned to the logged-in user with literacy status, transparency notices and linked Drive evidence files. Staff see what they are allowed to use and what disclosures apply — without access to registers they do not need to maintain.

Element	End-user information
literacyOk / literacyDue	Whether the user's literacy assignment is current.
notice	Transparency notice text applicable to the tool.
evidence	Linked files (policies, acceptable use) the user may consult.

24. Settings and reminders

AI Act settings (/business/ai-act/settings) exposes a manual reminder check and a link to product scope. Reminders are not legal deadlines — they are operational nudges deduplicated within seven days.

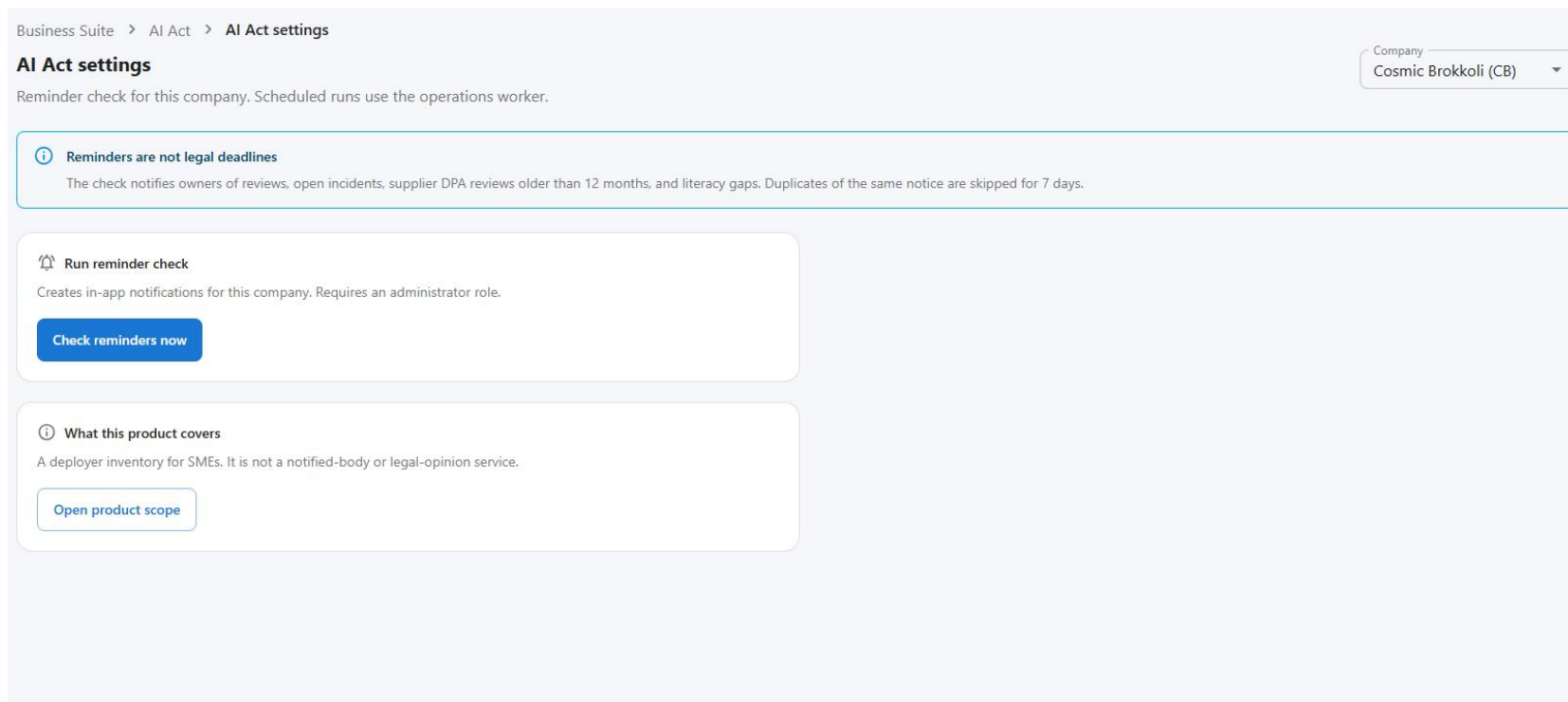


Figure 26 — AI Act settings — run reminder check and product scope link

- Systems with review_date within 7 days → notify owner.
- FRIA with review_date within 7 days → notify reviewer.
- Suppliers with no or stale last_review (>12 months) → notify fallback system owner.
- Open incidents → notify system owner.
- Assigned users without current literacy → notify employee and owner.

POST /api/v1/business/ai-act/check-reminders requires ADMIN role.

25. AI Act copilot (local Ollama)

The AI Act agent (AiActAgentGate) appears on all AI Act pages except My tools and About. It uses the same local copilot shell as the QMS agent: Ollama on the organisation's infrastructure, human confirmation for writes, and explicit disclosure that data stays on-premises.

 QMS agent

 Local AI system (Ollama). Data stays on-prem. Register changes require human confirmation. This is not a certification body.

Create a new risk about the security for developers working remotely and accessing to customer data

Checking QMS registers

Need a few details

qms.risks.create

1. Title of the risk or opportunity

2. Is this a risk or an opportunity?
RISK - OPPORTUNITY

3. Description (context, cause, effect)

4. Probability (1-5)

5. Impact (1-5)

1. Title of the risk or opportunity Remote Developer Data Access Security Risk

Fill the data with best bractices and give me a preview now before adding

Checking QMS registers

Using: qms.risks.create

Why: Creating a risk related to remote developer access to customer data with best practices in mind.

Need a few details

Ask the QMS agent...



Figure 27 — Local AI copilot shell — same UX for AI Act agent (AiActAgentWindow); writes require human Confirm

- Feature flags: AI_GATEWAY_ENABLED, AI_COPILOT_AIACT_ENABLED; Ollama must be reachable.
- APIs: /api/v1/ai/aiact/chat, /confirm, /health, /warmup.
- Read tools: overview, systems, FRIA, transparency, incidents, oversight, explanations, catalogues.
- Write tools: propose mutations; user must Confirm — same validation as UI forms.
- Not a legal adviser or notified body — answers may err; conformity decisions remain with competent persons.

26. Integrations with other NexusOS modules

Module	Integration
Drive	Evidence tab searches FILE nodes; My tools exposes clickable file links.
QMS (Quality)	DPIA evidence links QMS controlled documents via qmsNodeId; shared UI patterns (QaRegisterTable, activity feeds).
Employees	System Users tab and Literacy register share employee_literacy with Employee detail → Literacy tab.
Notifications	Reminder engine creates AIACT_FRIA_REVIEW, AIACT_SUPPLIER_REVIEW, AIACT_INCIDENT_OPEN, AIACT_LITERACY_DUE notifications.
Multi-tenant	Company selector; all codes and records scoped to tenant_id.

27. Product scope and limitations

The About page (/business/ai-act/about) documents controlled product boundaries. Auditors shall treat these as explicit scope statements:

27.1 What you can record

- Inventory of AI uses (SaaS tools and operational systems) with a working risk class.
- Art. 5 and Annex III as labels on the record — not a legal determination.
- FRIA, transparency notices, oversight, incidents and explanations as registers.
- Literacy assignments and reminders for people who use the tools.
- Evidence links to Drive files and, for DPIA, to QMS controlled documents.

27.2 What this product does not do

- Conformity assessment or a declaration that you comply with the AI Act.
- CE marking, Annex IV technical documentation or notified-body files.

- A provider quality management system if you place AI systems on the market.
- Filing in the EU database of high-risk systems.

Those duties need specialist legal advice and, where required, a different product or notified body.

28. Document control

This manual is controlled documented information. The current version is identified in the footer of every page after the cover. Superseded versions shall be withdrawn from operational use. Printed copies are uncontrolled unless stamped otherwise.

28.1 Revision history

Version	Date	Description	Prepared / updated by	Approved by
20260901.01	1 September 2026	Initial issue — NexusOS AI Act functional manual (regulatory context, all registers, gap engine, dossier, local copilot).	Marco Aveta / AI Act Coordinator	Stefania Aveta / CEO

End of controlled document. Cosmic Brokkoli UAB — Vilnius, Lithuania — <https://cosmicbrokkoli.com/>