VECTO

Autonomous Intelligence. Human Control.

AI Act Compliance

Hoe Vecto's architectuur EU AI Act-readiness ondersteunt

vecto-os.com · 5 May 2026

Samenvatting

De EU AI Act, afdwingbaar in de hele Europese Unie, verandert fundamenteel hoe organisaties AI-systemen moeten beheren. Voor elk team dat AI gebruikt in softwareontwikkeling, projectorkestratie of operationele workflows, introduceert de wet verplichtingen rond **risicoclassificatie, documentatie, traceerbaarheid, menselijk toezicht en post-market monitoring** die voorheen niet bestonden.

De meeste bestaande projectmanagement- en developertools zijn niet ontworpen met deze verplichtingen in het achterhoofd. Ze werden gebouwd toen "AI" een chatbot onderaan de pagina betekende — geen agent met de autoriteit om code te schrijven, sprints te plannen of productie-deployments te triggeren.

Vecto is anders gebouwd. Elke agent-actie wordt gelogd met volledige context. Elke beslissing is traceerbaar tot zijn oorsprong. Elke deployment draagt een chain-of-custody van idee tot release. Deze whitepaper legt uit hoe Vecto's architectuur aansluit bij de concrete verplichtingen van de EU AI Act, en hoe organisaties Vecto kunnen gebruiken als fundament voor hun compliance-houding.

1. De EU AI Act in Twee Pagina's

Wat het doet

De EU AI Act classificeert AI-systemen per **risico-tier** en legt verplichtingen op die proportioneel zijn aan die tier:

Tier	Voorbeelden	Vecto-relevante verplichtingen
Onacceptabel	Sociale scoring, real-time biometrische ID in publieke ruimte	Verboden
Hoog risico	AI in kritieke infrastructuur, werknemersbeslissingen, rechtshandhaving	Conformiteitsbeoordeling · Risicobeheer · Datagovernance · Documentatie · Menselijk toezicht · Accuraatheid, robuustheid, beveiliging · Post-market monitoring
Beperkt risico	AI die content genereert, chatbots, deepfakes	Transparantie (markeer als AI-gegenereerd)
Minimaal risico	Spamfilters, AI in spellen	Geen specifieke verplichtingen
GPAI (Algemeen doel)	Foundation models	Technische documentatie · Transparantie · Naleving EU-auteursrecht

Voor de meeste organisaties die AI gebruiken voor projectmanagement, code-generatie of operationele workflows, zijn de relevante tiers **Hoog risico** (wanneer AI-beslissingen werknemerspositie, kritieke operaties of gereguleerde sectoren beïnvloeden) en **Beperkt risico** (algemene productiviteits-AI).

Wat het vereist (de kern-verplichtingen)

Voor hoog-risico systemen moeten providers en deployers:

1. **Risicobeheersysteem** — continu, gedocumenteerd
2. **Datagovernance** — kwaliteit, representativiteit, bias-mitigatie
3. **Technische documentatie** — Annex IV minimum
4. **Logbeheer** — automatische logs van systeem-events
5. **Transparantie** — gebruiksinstructies, systeemlimieten
6. **Menselijk toezicht** — design maakt betekenisvolle menselijke controle mogelijk
7. **Accuraatheid, robuustheid, cybersecurity** — afgestemd op risico
8. **Post-market monitoring** — continue performance + incident-tracking

De wet treedt in fasen in werking gedurende 2026-2027. **Boetes lopen op tot €35 miljoen of 7% van de wereldwijde jaaromzet**, welke hoger is.

2. De Compliance-Last — Wat is Echt Nieuw

De meeste organisaties hebben al wel governance-praktijken. De AI Act voegt drie dingen toe die echt nieuw zijn:

a) Documentatie die het team overleeft

Annex IV vereist technische documentatie die uitlegt *waarom* het systeem werd gebouwd, *hoe* het beslissingen neemt, *welke* alternatieven werden overwogen, en *hoe* het wordt gemonitord. Deze documentatie moet geldig blijven gedurende de hele lifecycle van het systeem — niet alleen op certificeringsmoment.

De meeste tools kunnen geen cumulatieve, beslissings-verankerde documentatie produceren. Ze produceren tickets en commits, geen reasoning chains.

b) Menselijk toezicht als design-eigenschap

De wet vereist niet alleen menselijk toezicht in beleid. Het vereist dat het systeem zo **ontworpen** is dat menselijk toezicht betekenisvol is. Dat betekent dat agents moeten opereren op een duidelijk gedefinieerd autonomie-niveau, met menselijke interventiepunten, met de mogelijkheid om te stoppen, override te plegen of te auditen.

De meeste AI-tools werken vandaag als black boxes met één enkel autonomie-niveau. Ze laten je niet tunen hoeveel autoriteit de AI heeft per taak of per project.

c) Audit trail als first-class concern

Voor hoog-risico systemen moet elke systeem-event automatisch worden gelogd met voldoende detail om te reconstrueren wat er is gebeurd. Niet “we hebben ergens logs”. Gestructureerd, immutable, exporteerbaar, traceerbaar tot de actor (mens of agent).

De meeste logging gebeurt op applicatieniveau, niet op actorniveau. Het vertelt je *wat* er is gebeurd, niet *wie* (of *welke agent*) het deed, *met welke autoriteit*, en *gebaseerd op welke voorafgaande beslissing*.

---

3. Vecto’s AI-Governance Architectuur

Vecto is gebouwd op drie architecturale keuzes die deze nieuwe vereisten direct adresseren:

3.1 De Levende Graph

Elk artefact in Vecto — elk idee, beslissing, plan, taak, deployment, incident — is een node in een typed graph. Elke relatie tussen artefacten is een typed edge. Dat betekent:

- Beslissingen wijzen naar de problemen die ze oplosten
- Plannen wijzen naar de incidenten die ze triggerden
- Code-changes wijzen naar de user stories die ze motiveerden
- Releases wijzen naar de security reviews die ze goedkeurden

De graph is de documentatie. Annex IV-stijl technische documentatie kan **afgeleid** worden uit de graph op elk moment in de tijd — automatisch, compleet, en traceerbaar.

3.2 Het Autonomie-Spectrum

Elke Vecto-agent werkt op een configureerbaar autonomie-niveau, van `Observe` (alleen-lezen audit) tot `Automate` (volledige autonomie). Het niveau kan ingesteld worden per project, per gebruiker, per taaktype. Dit geeft compliance-teams een concreet, meetbaar antwoord op "hoeveel menselijk toezicht is in dit systeem ingebouwd?"

Niveau	Menselijke rol	AI-autoriteit
Observe	Beslisser	Alleen rapporteren
Advise	Beslisser	Suggereert opties
Assist	Reviewer	Handelt na goedkeuring
Delegate	Kader-zetter	Handelt binnen kaders
Automate	Auditor	Handelt zelfstandig (zeldzaam, by design)

De default is `Assist`. `Automate` wordt expliciet als uitzonderlijk gemarkeerd.

3.3 Cryptografisch Verankerd Audit Trail

Elke agent-actie emit een audit-event met: actor-identiteit (mens of agent), timestamp, scope (welke workspace), actie-categorie, gevoeligheid, severity, en een referentie naar de beslissings-context die het autoriseerde. Audit-events zijn immutable, exporteerbaar, en getekend. **Releases dragen HMAC-getekende sign-off-ketens** die het oorspronkelijke idee koppelen aan het deployed artefact.

Dit is geen afterthought logging-laag. Het is een kern-datastructuur.

---

4. Hoe Vecto Mapt op AI Act Artikelen

AI Act verplichting	Vecto capability
Art. 9 — Risicobeheersysteem	Risico-register als graph nodes; beslissingen wijzen naar risico's; periodieke risico-review ingebouwd in release flow
Art. 10 — Datagovernance	Data lineage via graph edges; databronnen gedocumenteerd per node
Art. 11 — Technische documentatie	Auto-gegenereerd uit graph; afgestemd op Annex IV outline
Art. 12 — Logbeheer	Immutable audit log per actor + actie; cryptografische integriteit
Art. 13 — Transparantie	Agent-capabilities gepubliceerd per autonomie-niveau; gebruiksinstructies ingebouwd in onboarding
Art. 14 — Menselijk toezicht	Autonomie-spectrum design; expliciete sign-off gates per release; interventie altijd beschikbaar
Art. 15 — Accuraatheid, robuustheid, cybersecurity	TLS 1.3 transport, AES-256 at rest, RBAC, tenant-isolatie, getekende releases
Art. 26 — Deployer-verplichtingen (logging)	Alle logs exporteerbaar; post-market monitoring data automatisch geproduceerd
Art. 73 — Ernstige incident-rapportering	Incident node-type met timestamp, severity, en link naar getriggerde beslissingen

Dit is geen 100% turnkey AI Act-oplossing. **Het is de fundamentele data-architectuur waarop een compliant programma gebouwd wordt.** Gecombineerd met passend organisatiebeleid reduceert Vecto de documentatie- en traceerbaarheidslast aanzienlijk.

5. Documentatie die Annex IV vraagt (en Vecto auto-genereert)

Annex IV vereist:

1. Algemene beschrijving van het AI-systeem
2. Gedetailleerde beschrijving van elementen + ontwikkelproces

3. Informatie over monitoring, functioneren, controle
4. Beschrijving van risicobeheersysteem
5. Beschrijving van wijzigingen gedurende de lifecycle
6. Lijst van toegepaste geharmoniseerde standaarden
7. Kopie van EU-conformiteitsverklaring
8. Beschrijving van het post-market monitoring-systeem

Van deze items zijn **2, 3, 5 en 8** documentatie die traditioneel handmatig schrijven en onderhoud vereisen. In Vecto zijn ze **outputs van de graph zelf**:

- Item 2 (ontwikkelproces) → afleidbaar uit de keten van IDEAs → EPICs → STORIES → TASKS → RELEASES
- Item 3 (monitoring + controle) → afleidbaar uit autonomie-niveau-configuratie + audit-trail-volledigheidsrapporten
- Item 5 (wijzigingen gedurende lifecycle) → de graph is, per definitie, een chronologisch register van wijzigingen
- Item 8 (post-market monitoring) → afleidbaar uit incident-node-aggregatie + auto-gegenereerde KPI-dashboards

Dit is het verschil tussen *documentatie schrijven* en *documentatie exporteren*.

---

6. De Vecto Compliance-Checklist

Gebruik deze checklist om elke AI-tool te evalueren tegen AI Act-readiness — inclusief Vecto:

Traceerbaarheid

- [ ] Elke AI-actie wordt gelogd met actor-identiteit
- [ ] Logs zijn immutable en tamper-evident
- [ ] Logs zijn exporteerbaar in machine-leesbaar formaat
- [ ] Beslissingen kunnen getraced worden van outcome terug naar oorspronkelijke context

Menselijk toezicht

- [ ] AI-autoriteit is configureerbaar per taak / project / gebruiker
- [ ] Menselijke interventiepunten zijn ontworpen in de workflow
- [ ] AI kan menselijke review niet omzeilen voor safety-kritieke beslissingen
- [ ] Operators kunnen AI-acties in real time overrulen of stoppen

Documentatie

- [ ] Technische documentatie kan op elk moment opnieuw gegenereerd worden
- [ ] Documentatie bevat de *reasoning* achter beslissingen, niet alleen outcomes
- [ ] Wijzigingen gedurende lifecycle worden vastgelegd met context
- [ ] Documentatie is geen snapshot — het is een levend artefact

Datagovernance

- [ ] Databronnen zijn gedocumenteerd per AI use case
- [ ] Data lineage van input naar output is traceerbaar
- [ ] Bias- en kwaliteitsbeoordelingen worden vastgelegd

Beveiliging

- [ ] Encryptie in transit (TLS 1.3+) en at rest (AES-256)
- [ ] Multi-tenant isolatie op databaseniveau, niet alleen applicatieniveau
- [ ] Access control is role-based en least-privilege by default
- [ ] Secrets zijn versleuteld met roteerbare sleutels

Post-market monitoring

- [ ] Systeem-events voeden een geaggregeerde monitoring-view
- [ ] Incidents kunnen automatisch worden gecategoriseerd op severity
- [ ] Performance-metrics worden over tijd getracked
- [ ] Rapporten kunnen on demand gegenereerd worden voor regulators

Als je vandaag de meeste van deze vinkjes niet kan zetten, sta je voor significant werk om AI Act-readiness te bereiken. Vecto biedt deze checklist als fundament, niet als de hele oplossing.

---

7. Wat Vecto NIET Doet

Om transparant te zijn over scope:

- Vecto is **geen** AI Act-certificering. Conformiteitsbeoordeling vereist in veel gevallen een notified body.
- Vecto **vervangt** je DPO, je CISO of je compliance-team niet. Het ondersteunt hen.

- Vecto classificeert **niet automatisch** de risico-tier van je AI-systeem. Dat vereist legal + business judgment.
- Vecto's audit trail is **noodzakelijk maar niet voldoende** voor volledige Annex IV-documentatie. Het is het fundament, niet het complete document.

We positioneren Vecto als de **infrastructurele ruggengraat** voor AI-governance. Het organisatorische, juridische en beleidswerk blijft van jou — maar het technisch bewijs is auto-gegenereerd, traceerbaar en exporteerbaar.

---

8. Over Vecto

Vecto is een graph-native projectplatform gebouwd voor organisaties die AI-governance serieus nemen. We zijn gevestigd in België, met EU-soevereiniteit als kern-architecturale keuze. Ons platform is beschikbaar als public SaaS, private SaaS, on-prem, en (gepland) fysieke appliance.

Opgericht in 2026 door een team met achtergronden in cryptografie, enterprise security, AI-orkestratie en product delivery. Foundation-led governance zorgt dat de missie van het platform niet kan worden verwaterd of weggekocht.

Voor demo, evaluatie of compliance-gesprek: **vecto-os.com**

Deze whitepaper is informatief, geen juridisch advies. Raadpleeg gekwalificeerd juridisch advies voor AI Act-conformiteitsbeoordeling specifiek voor jouw context.