



Vlaanderen  
is ondernemen

# LISA: LLM Implementation, Security & Adaptation

AANVRAAG COOCK+

# Opmaak en samenstelling van de projectaanvraag

## 1. Checklist

schrappen wat niet van toepassing is

DEEL A: Steun aan Onderzoeksorganisaties

DEEL 0: PROJECTBEGROTING

Overzicht totale projectbegroting

DEEL 1: PROJECTIDENTIFICATIE

Algemeen doel

Herindiening

Gegevens van de leden van de begeleidingsgroep

DEEL 2: PROJECTBESCHRIJVING

Doelstellingen

Fit in het programma

Werkplan

Middelen en expertise

Economisch impact

Kennisverspreiding

Ruimere meerwaarde

Afzonderlijk in het onlineportaal op te laden

Excel-file met begroting per partner en gezamenlijke begroting (verplicht)

Verklaring van Organisatie voor Onderzoek en Kennisverspreiding

Offertes (of factuur van eerdere bestellingen of gemotiveerde kostenschatting) ter onderbouwing van de kost voor onderaannemingen vanaf € 10.000 (verplicht indien van toepassing)

Bijlage m.b.t. de clusterspecifieke en/of transitieprioriteiten criteria (indien van toepassing)

**Andere bijlagen worden niet beschouwd.**

Trefwoorden

Geef op:

- *4 sleutelwoorden: Large Language Models, AI security, DevOps, Governance*
- *Economische sector: Software Development (early adopters)*
- *Onderzoeksdomein: Veilig beheer van LLM-technologie*

## Deel 0: Projectbegroting

2 VLAIO COOCK+ Aanvraagtemplate – versie maart 2024 - VERTROUWELIJK

VLAIO.be

# Deel 1: Projectidentificatie

## 1. Algemeen doel

De opkomst van Large Language Models (LLM's) brengt nieuwe mogelijkheden met zich mee voor softwareontwikkelaars om geavanceerde functionaliteiten te implementeren die tot voor kort onmogelijk waren. Krachtige taalmodellen, zoals GPT4 en LLama2/3, stellen ontwikkelaars in staat om complexe 'Natural Language Processing'-taken op een gemakkelijker manier te integreren. Ze kunnen toegepast worden in allerlei scenario's, gaande van metadata-extractie uit documenten tot semantische zoekopdrachten op basis van embedding sen alternatieve conversationele gebruikersinterfaces (in de plaats van klassieke 'wizards'). Het is dan ook niet verwonderlijk dat softwarebouwers volop experimenteren met LLM's om deze geavanceerde gebruiksscenario's te implementeren. De beschikbaarheid van open-source modellen, bibliotheken en services maakt deze technologie toegankelijk voor iedereen met basiskennis van programmeren.

Echter, naast de mogelijkheden zijn er ook uitdagingen. Het bouwen van Proof of Concepts met LLM's is vandaag triviaal, maar klassieke kwaliteitseisen zoals performantie, kosten, betrouwbaarheid en veiligheid mogen niet overboord worden gegooid (bedrijven kunnen zich niet permitteren om zaken zoals ... overboord te gooien). Lessons learned uit softwareproductontwikkeling en DevOps moeten opnieuw worden geïnterpreteerd en aangepast worden wanneer LLM's een deel van de software aandrijven.

In het LISA-project willen Sirris en DistriNet de best practices uit software engineering en DevOps vertalen naar softwareteams die LLM's op een veilige manier in hun toepassingen willen gebruiken. Naast de integratie en het testen van LLM's, wordt een sterke focus gelegd op de maatregelen die moeten getroffen worden om misbruik van het systeem door derden te vermijden. We houden de vinger aan de pols van de evoluties in dit opkomende veld en bieden praktische voorbeelden, aanbevelingen en inzichten.

Momenteel is er een aanzienlijke nood aan kennis om deze nieuwe technologieën effectief te integreren. Ondanks het gebrek aan diepgaande kennis, investeren early adopters volop in nieuwe *generative AI* (genAI)-mogelijkheden omdat ze het potentieel van deze technologieën onderkennen. Dit plaatst hen echter in een kwetsbare positie als achteraf blijkt dat ze de risico's die gepaard gaan met dergelijke systemen hebben onderschat. Dit project tracht deze bedrijven te behoeden voor onvoorziene problemen of zelfs juridische complicaties die kunnen ontstaan door onzorgvuldige implementatie.

Het is duidelijk dat genAI-technologieën, met LLM's in de voorhoede, baanbrekend zijn. Het staat vast dat consumenten steeds vaker in aanraking zullen komen met dergelijke geavanceerde toepassingen in de toekomst. Het potentieel van Large Language Models om complexe taalkundige taken te automatiseren en te verbeteren zal toepassingen kennen in een breed scala aan industrieën. Onrechtstreeks zal dit project dus een brede impact hebben binnen de Vlaamse economie.

## 2. Herindiening

Dit project is geen herindiening.

### 3. Gegevens van de leden van de begeleidingsgroep en van reeds geïdentificeerde intenties tot ondernemingsspecifieke acties

Organisatie	Toegezegd	Vlaamse KMO	Schakel in de waardeketen	Intensie voor OSA	Categorie
Xenit	ja	ja	softwarebouwer	ja	document management
Proplanner	ja	ja	softwarebouwer	ja	fleetmanagement
Impaqtr	ja	ja	softwarebouwer	ja	Data platform
Quasidoc	ja	ja	softwarebouwer	ja	ERP en kwaliteitsbewaking
Flagstone	ja	ja	softwarebouwer	ja	MES
Arkite	ja	ja	softwarebouwer	ja	operator support
Gim	ja	ja	softwarebouwer	ja	GIS
azumuto	ja	ja	softwarebouwer	ja	operator support
Barco	ja	neen	softwarebouwer	ja	medical
axi	ja	neen	integrator	ja	integrator
fitme.jobs	ja	ja	SaaS provider	ja	hr
Televic Group	ja	neen	softwarebouwer	ja	rail, education
Cognit	ja	ja	softwarebouwer	ja	content management
Youston	ja	ja	softwarebouwer	ja	document management
The Talentbox	ja	ja	SaaS provider	ja	HR
Axians	ja	neen	integrator	ja	energie, manufacturing
King and Queen Journeys	ja	ja	integrator	ja	Startups
Play it	ja	ja	SaaS	ja	HR, play-based learning
UpdatePro	Ja	Ja	Digitaal uitzendkantoor	Ja	HR

Onderneming	Xenit
Beschrijving onderneming en voornaamste activiteiten	Xenit is een bedrijf dat actief is in document management
Ondernemingsnummer (voor Belgische organisaties) of adres	BE 0887.582.365
Naam van de contactpersoon en functie	Ronny Timmermans, CEO
Tel en e-mail	
Vlaamse kmo? (zie definitie in de handleiding)	Ja
Bereid tot deelname begeleidingsgroep	Ja
Intentie ondernemingsspecifieke actie	Ja

Als bedrijf dat actief is in document management, weet Xenit als geen ander hoe moeilijk het soms is om met ongestructureerde, tekstuele data om te gaan. Het bedrijf gebruikt al jaren allerhande op NLP (natural language processing) gebaseerde technieken om meta-data af te leiden uit de documenten die het via haar platformen verwerkt.

Met de toenemende populariteit van large language models, experimenteert Xenit volop hoe het deze modellen kan inzetten om een generiekere manier dan vandaag, allerhande meta-data uit die documenten te halen. Ook de "chat met uw documenten" use-case wordt volop ge-exploereerd. Het bedrijf heeft daartoe al verschillende experimenten en proof-of-concepts lopen.

Hoewel deze experimenten veelbelovend zijn, heeft Xenit toch nog een heleboel vragen rond het gebruik van llms in hun software, zoals:

- Hoe omgaan met hallucinaties van het model? Hoe dit evalueren tijdens development en in productie?
  - o Hoe loggen we slechte responses en hoe voeden we die terug?
- Voor chat use-cases: hoe beschermen we onze applicatie tegen prompt injection?
- Portability: Xenit gebruikt soms "function calling", maar niet alle llm-vendors bieden dit aan. Hoe vermijden we vendor lock-in?
- Llms gebruiken is duur: hoe houden we kosten onder controle en hoe kunnen we kosten vs. benefits afwegen, zowel tijdens ontwikkeling als in productie?
- Wat met de huidige en toekomstige wetgeving zoals GDPR, de AI act? In hoeverre beïnvloedt de wetgeving ons gebruik van (bepaalde) llms?

Xenit verwacht dat ze met een deelname aan LISA ervaring kan opdoen en uitwisselen met het project en de andere leden van de stuurgroep. Xenit hoopt ook inzicht te krijgen in hoe llm-gebaseerde applicaties te monitoren, zowel tijdens development (testing) als in productie.

*Ronny Timmermans*

Ronny  
Timmerman  
s (Signature)  
  
 Digitaal  
ondertekend door  
Ronny Timmermans  
(Signature)  
 Datum: 2024.05.28  
 17:57:04 +02'00'

Onderneming	ProPlanner	
Beschrijving onderneming en voornaamste activiteiten	Fleet management software voor verhuurbedrijven en garages	
Ondernemingsnummer (voor Belgische organisaties) of adres	0825.043.990	
Naam van de contactpersoon en functie	Jeroen Vanreybrouck – CTO	
Tel en e-mail	0472 79 13 14	Jeroen.vanreybrouck@proplanner.eu
Vlaamse kmo? (zie definitie in de handleiding)	Ja	
Bereid tot deelname begeleidingsgroep	Ja	Nee
Intentie ondernemingsspecifieke actie	Ja	Nee
<p>Proplanner bouwt gebruiksvriendelijk fleetsoftware die cardealer of autoverhuurbedrijven ondersteunt bij het uitlenen, verhuren en optimaal inzetten van voertuigen en accessoires.</p> <p>Vandaag gebruikt Proplanner nog geen generatieve AI of large language models, al krijgt het van haar klanten wel de vragen in die richting. Het bedrijf is zich nog volop aan het oriënteren en verwacht in de toekomst wel llm-gebaseerde functionaliteit te gaan aanbieden. AI heeft het bedrijf daarbij nog vele vragen: wat met hallucinaties? Hoe kunnen we ervoor zorgen dat de outputs ten allen tijden geoorloofd zijn en wat met de toch wel hoge kosten?</p> <p>Via een deelname aan de gebruikersgroep van LISA hoopt Proplanner beter geïnformeerde beslissingen te nemen rond haar toekomstige investeringen in llm technologie. Het bedrijf kijkt uit naar demonstratoren en best practices die haar kunnen helpen versneld en veilig de voordelen van llms te kunnen benutten.</p>		

Naam & Handtekening

Datum: 04/06/2024

Jeroen Vanreybrouck



Onderneming	IMPAIGT NV	
Beschrijving onderneming en voornaamste activiteiten	<p>We developed the SaaS platform Amora to structure and distribute insights in a data ecosystem. We develop high end productivity insights for retail and manufacturers.</p>	
Ondernemingsnummer (voor Belgische organisaties) of adres	BE 0876 205 887	
Naam van de contactpersoon en functie	Bart Jacobs (founder & CEO)	
Tel en e-mail	0477/687407	bart.jacobs@impagt.com
Vlaamse kmo? (zie definitie in de handleiding)	(Ja) nee (indien nee, aard organisatie toevoegen)	
Bereid tot deelname begeleidingsgroep	<input checked="" type="checkbox"/> Ja	Nee
Intentie ondernemingsspecifieke actie	<input checked="" type="checkbox"/> Ja	Nee
<ol style="list-style-type: none"> <li>1. Bondige motivatie van de onderneming of non-profitorganisatie tot deelname aan de begeleidingsgroep. <i>Bondmark our own AI pilot with others.</i></li> <li>2. De kennissprong die de onderneming verwacht te verwerven dankzij deel A van het COOCK+-project. <i>less continuous automation and efficiency</i></li> <li>3. Toelichting bij de intentie tot het nemen van een ondernemingsspecifieke actie. <i>Roll out of our first AI driven module</i></li> </ol>		

Naam & Handtekening



Bart Jacobs

Datum:

28/05/2024

Onderneming	Quasydoc BV	
Beschrijving onderneming en voornaamste activiteiten	QuaSyDoc – Bouwer van ERP en kwaliteitsbewakingssoftware voor de voedingsindustrie.	
Ondernemingsnummer (voor Belgische organisaties) of adres	BE 0660.744.006 Herkenrodesingel 4 bus 2, 3500 Hasselt.	
Naam van de contactpersoon en functie	Johan Vandercappellen, Bestuurder	
Tel en e-mail	+32 (0) 479/79.07.82	<a href="mailto:Johan@Quasydoc.eu">Johan@Quasydoc.eu</a>
Vlaamse kmo? (zie definitie in de handleiding)	Ja/nee (indien nee, aard organisatie toevoegen)	
Bereid tot deelname begeleidingsgroep	Ja	Nee
Intentie ondernemingsspecifieke actie	Ja	Nee

QuaSyDoc BV bouwt Saas-software voor de voedingsindustrie. Op basis van de QuaSyDoc software beheren voedingsbedrijven de kwaliteit en voedselveiligheid van hun producten en processen. QuaSyDoc is zeer geïnteresseerd in de ontwikkelingen die gebeuren in het domein van large language models (LLM's), maar heeft op dit moment onvoldoende expertise in huis om er mee aan de slag te gaan.

In het algemeen kan de integratie van LLM-technologie in incidentrapportageprocessen de efficiëntie, nauwkeurigheid en besluitvorming binnen beheersystemen voor voedselveiligheid verbeteren. We denken hierbij aan volgende mogelijke toepassingen:

- **Documentatie en rapportage:** LLM's kunnen helpen bij het genereren van gestructureerde incidentrapporten, samenvattingen en vervolgacties op basis van de verstrekte informatie, waardoor het documentatieproces wordt gestroomlijnd.
- **Geautomatiseerde gegevensanalyse:** Quasydoc bevat een hele reeks kwaliteitsdata van haar klanten. Dit betreft zowel kwantitatieve data, zoals analyseresultaten, als kwalitatieve data zoals incidentmeldingen. We zijn geïnteresseerd om verder uit te zoeken hoe LLM's deze data kunnen omzetten tot voor de klant relevante informatie.
- **Trendidentificatie:** Door een groot aantal incidentmeldingen te verwerken, kunnen LLM's patronen en trends identificeren die mensen misschien niet zo snel opmerken. Dit kan helpen bij het opsporen van terugkerende problemen en het implementeren van preventieve maatregelen.
- **Begrijpen van natuurlijke taal:** LLM's kunnen tekst in natuurlijke taal begrijpen, waardoor gebruikers incidentgegevens op een converserende manier kunnen invoeren. Dit vereenvoudigt het rapportageproces en zorgt ervoor dat alle benodigde informatie wordt vastgelegd.
- **Risicobeoordeling:** LLM's kunnen helpen bij risicobeoordeling door incidentrapporten en andere relevante gegevens te analyseren om potentiële risico's te beoordelen en prioriteiten te stellen voor corrigerende maatregelen.

- **Aanbevelingen en best practices:** Op basis van de analyse van incidentrapporten kunnen LLM's aanbevelingen doen voor het verbeteren van voedselveiligheidspraktijken, het implementeren van best practices en het voorkomen van toekomstige incidenten.
- **Etikettering van voorverpakte levensmiddelen:** De QuaSyDoc software biedt de mogelijkheid om de voor levensmiddelen wettelijk verplichte informatie voor de consument automatisch te genereren op basis van recepten en info van de leveranciers: etiketten op voedingswaren te beheren, te vertalen en te toetsen aan (internationale) wetgeving. Mogelijk kan LLM-technologie hier een significante meerwaarde betekenen. Deze meerwaarde zal echter alleen gerealiseerd kunnen worden als QuaSyDoc de nodige garanties kan geven naar correctheid van vertalingen e.d. Het soms wispeturige karakter van LLM's (hallucinaties, niet altijd even deterministisch) zijn op dit moment redenen om nog niet aan de slag te gaan met LLM's.
- **Beoordeling van leveranciersspecificaties automatiseren:** Via Quasydoc kunnen voedingsbedrijven productinformatie verzamelen bij hun leveranciers. LLM's kunnen mogelijk ondersteunen bij het bepalen van welke info relevant is voor een bepaalde productgroep enerzijds en bij de interpretatie/beoordeling van de door de leverancier verstrekte informatie anderzijds.
- ... (Ongetwijfeld zullen we tijdens dit traject een hele reeks andere mogelijkheden ontdekken.)

Gezien deze thema's aan bod zullen komen in het LISA project, ziet QuaSyDoc via deelname aan de gebruikersgroep een opportuniteit om versneld en op basis van praktijkvoorbeelden, beter te kunnen inschatten hoe het bedrijf llm technologie veilig en robust kan inzetten binnen haar softwarepakketten.

Naam & Handtekening

ir. Johan Vandercappellen

Johan  
Vandercappellen  
(Signature)

Digitaal ondertekend door  
Johan Vandercappellen  
(Signature)  
Datum: 2024.05.24 19:32:33  
+02'00'

Datum:

24/05/2024

Onderneming		
Beschrijving onderneming en voornaamste activiteiten	Flagstone – Bouwer van MES systemen	
Ondernemingsnummer (voor Belgische organisaties) of adres	BE0635.607.445	
Naam van de contactpersoon en functie	Jurgen Dekeyser	
Tel en e-mail	056/98.07.98	jurgen@flagstone.Tech
Vlaamse kmo? (zie definitie in de handleiding)	Ja/nee (indien nee, aard organisatie toevoegen)	
Bereid tot deelname begeleidingsgroep	Ja	Nee
Intentie ondernemingsspecifieke actie	Ja	Nee
<p>Flagstone is een kmo die MES (manufacturing execution system) software bouwt. De Flagstone software verrijkt de productiedata door middel van data uit machines, ERP data en operator data, om zo een maximale ondersteuning te bieden aan de arbeiders door middel van real-time order informatie, werkinstructies, machine instellingen, kwaliteitstesten en doelstellingen.</p> <p>Flagstone maakt op dit moment nog geen gebruik van large language models en generatieve AI, al bekijkt het de deze technologische evolutie met argusogen. Volgende cases zijn vormen mogelijk voor hun klanten een meerwaarde:</p> <ul style="list-style-type: none"> <li>○ Last mile bijsturen van orders op bepaalde werkposten (dus het verschuiven van orders adhv bepaalde situaties of preventie van bepaalde productiestoringen door vb te anticiperen op data events zoals: stoppen van een conveyor belt, stilstaan van AGV, etc...)</li> <li>○ Kwaliteitsborging: de ideale situatie is preventie van out of spec situaties. Geavanceerde opvolging van operator ingegeven informatie; correlaties van afwijkingen van het verleden op een machine lijn voortvloeiend op potentiële deviaties kunnen zorgen dat er al advies komt wat er dient te gebeuren om te voorkomen dat je out of spec krijgt</li> <li>○ Wij tonen events (zelfde als een belletje in facebook) waarin de melding wordt gegeven: een operator weet echter dan nog niet wat hij moet doen...dus net als stap hieronder vanuit de data informatie kunnen tonen in bepaalde situaties zorgt voor een snellere heropstart van de lijn</li> <li>○ Werkinstructies</li> <li>○ Complexer bevragen via NLP tov info van het verleden: "geef mij een overzicht van..."; "hoeveel producten werden uitgeleverd geproduceerd op deze machine op dat tijdstip....",...</li> </ul>		

Echter, gezien de kritische aard van de Flagstone software (het operationeel ondersteunen van manufacturing processen, waarbij elke fout of stilstand letterlijk uitgedrukt wordt in euro's), is het bedrijf terughoudend om al meteen aan de slag te gaan met llm's. De vrees dat hallucinaties operatoren foute informatie zou doorgeven, of dat de kostprijs van een llm-gebaseerde oplossing te hoog zouden zijn, zijn slechts enkele van de bezorgdheden van het team.

Flagstone verwacht echter door deel te nemen aan de gebruikersgroep van LISA, duidelijke inzichten te krijgen hoe op een betrouwbare en robuste manier llm technologie te kunnen inzetten. Deze kennis zal door het bedrijf ingezet worden om een beter gefundeerde beslissingen te nemen naar zin of onzin van llms voor hun eigen use cases.

Naam & Handtekening

Jeroen Donoyson



Datum:

24/05/2024

Onderneming	Arkite	
Beschrijving onderneming en voornaamste activiteiten	<p>Arkite biedt een operator guidance oplossing aan met behulp van augmented reality. Operatoren in de maakindustrie worden met behulp van Arkite begeleid in hun proces. De software voorziet een intuïtieve user interface om deze begeleiding in te stellen per werkstation.</p>	
Ondernemingsnummer (voor Belgische organisaties) of adres	BE0865543569	
Naam van de contactpersoon en functie	Bart Lamberigts, CTO	
Tel en e-mail	<a href="mailto:Bart.lamberigts@arkite.com">Bart.lamberigts@arkite.com</a>	+32496574596
Vlaamse kmo? (zie definitie in de handleiding)	Ja/nee (indien nee, aard organisatie toevoegen)	
Bereid tot deelname begeleidingsgroep	Ja	Nee
Intentie ondernemingsspecifieke actie	Ja	Nee
<p>Arkite is een softwarebedrijf dat gespecialiseerd is in het aanbieden van operator ondersteuning. Via de Arkite oplossing worden instructies geprojecteerd op de werkplek, zodat operatoren efficiënter kunnen werken.</p> <p>Vandaag gebruikt Arkite nog geen large language modellen in haar software, al ziet het zeker de mogelijkheden. Zo zouden llms kunnen gebruikt worden ter ondersteuning van het maken van nieuwe werkinstructies. Arkite heeft evenwel vele vragen bij de correctheid van de outputs van de llms, en vraagt zich ook af hoe de llm-gebaseerde functionaliteit aan te bieden aan de gebruikers, op zo'n manier dat de gebruiker ten allen tijden de eindvalidatie doet van de llm-outputs.</p> <p>Met haar deelname aan LISA verwacht Arkite zich een genuanceerd beeld te kunnen vormen over de mogelijkheden en uitdagingen die llm-technologie met zich meebrengt. Het bedrijf is sterk geïnteresseerd om een overzicht te krijgen van de veel-voorkomende use cases en de daaraan verbonden risico's. Ook validatietechnieken die de veiligheid en robustheid van llm-gebaseerde features moet bewaken, zijn thema's waarin Arkite geïnteresseerd is.</p>		

Naam & Handtekening

Datum: 05/06/2023

Bart Lamberigts



- - - - -

Onderneming	G.I.M.-Geographic Information Management NV	
Beschrijving onderneming en voornaamste activiteiten	<p>GIM, deel van de Merkator groep, werd opgericht in 1994 en is een toonaangevende Belgische leverancier van geodata-integratie, Geo-AI en Geo-ICT-oplossingen. Met een team van meer dan 70 geo-experts helpt GIM bedrijven, overheden en nutsbedrijven om slimmere beslissingen te nemen en vlotter te werken. GIMs vlaggenschip Belmap, de digitale versie van de leefomgeving, biedt heldere inzichten in alle gebouwen, adressen en aanverwante thema's in de Benelux.</p>	
Ondernemingsnummer (voor Belgische organisaties) of adres	BE 0454 064 819	
Naam van de contactpersoon en functie	Steven Smolders, Bestuurder en CTO	
Tel en e-mail	0498/976843	Steven.smolders@gim.be
Vlaamse kmo? (zie definitie in de handleiding)	Ja	
Bereid tot deelname begeleidingsgroep	Ja	
Intentie ondernemingsspecifieke actie	Ja	
<p>GIM is een bedrijf gespecialiseerd in geografische data (GIS). Het bedrijf bouwt een aantal softwareproducten waarmee het GIS data ontsluit van haar klanten. Daarnaast bouwt GIM data producten zoals Belmap.be. GIM heeft ruime ervaring in Computer Visie en Predictive modelling AI technieken.</p> <p>GIM experiment vandaag volop met large-language-models en copilots ter ondersteuning van de interne software-ontwikkelingsprocessen. Daarnaast krijgt het meer en meer vragen van klanten om (een deel van) hun GIS data te ontsluiten via natural language interfaces.</p> <p>Een deelname aan LISA zou voor GIM betekenen dat we versneld inzicht krijgen in de volledige kost, zowel qua ontwikkeling als operationeel, om een werkend IIm-gebaseerd systeem te bouwen. Elementen zoals veiligheid, betrouwbaarheid en robustheid zijn immers voor GIM en haar klanten van groot belang.</p> <p>Daarnaast kijkt GIM ook in de richting van "prompt-based" configureren van workflows binnen haar software. Veiligheid is in zo'n use case zeker van belang, omdat 'function calling' mogelijk de deur openzet tot het uitvoeren van "arbitraire code".</p>		

Naam & Handtekening

Datum: 04/06/2024

Permanent representative  
iogeo bv, director G.I.M. -  
Geographic Information  
Management NV

Onderneming	Azumuta	
Beschrijving onderneming en voornaamste activiteiten	Platform for the Connected Worker. Digital work instructions, embedded quality checklists, competency management, digital audits & checklists, data insights.	
Ondernemingsnummer (voor Belgische organisaties) of adres	BE 0667.713.356	
Naam van de contactpersoon en functie	Batist Leman	
Tel en e-mail	+32 499 34 60 69	batist.leman@azumuta.com
Vlaamse kmo? (zie definitie in de handleiding)	Ja	
Bereid tot deelname begeleidingsgroep	Ja	Nee
Intentie ondernemingsspecifieke actie	Ja	Nee
<p>Azumuta bouwt een software platform dat frontline workers ondersteunt rond zaken als regulatory compliance, werkinstructies en dergelijke.</p> <p>Azumuta heeft vandaag al proof-of-concepts gebouwd waarmee het, in samenspraak met lead users, reeds aantoont dat het, dankzij generatieve AI, klanten kan helpen met het sneller en beter aanmaken van werkinstructies. Azumuta ziet daarenboven nog meerdere potentiële use cases voor large language model technologie in haar platform.</p> <p>Het doen van deze proof-of-concepts heeft Azumuta geleerd dat het niet altijd even eenvoudig is om een robuuste en correcte output te genereren, en dat er behoorlijke uitdagingen zijn in het testen en blijvend valideren van de llm-gebaseerde oplossingen. Ook de snelle evolutie van de modellen wordt gezien als zowel een goede zaak (krachtigere modellen, bredere inzetbaarheid) als een risico (elk model heeft eigen karakteristieken, die niet altijd even eenvoudig te valideren zijn binnen de eigen use case).</p> <p>Met een deelname aan de gebruikersgroep van LISA verwacht Azumuta versneld de nodige inzichten op te doen in dit domein. Azumuta verwacht dat het aan de hand van de demonstratoren beter zal kunnen inschatten hoe het op een veilige manier het volle potentieel van llms zal kunnen benutten.</p>		

Naam & Handtekening

Datum: 2024-06-05

Batist Leman



Onderneming	<b>Barco NV</b>	
Beschrijving onderneming en voornaamste activiteiten	<b>Barco NV is een Belgisch technologiebedrijf, wereldwijd actief in drie markten: Healthcare (visualisatie van medische beeldvorming), Enterprise (grote video-muren en draadloze presentatiesystemen) en Entertainment (projectiesystemen voor cinema).</b>	
Ondernemingsnummer (voor Belgische organisaties) of adres	<b>BE 0473.191.041 Beneluxpark 21, 8500 Kortrijk</b>	
Naam van de contactpersoon en functie	<b>Elie De Brauwer - Software Architect</b>	
Tel en e-mail	<b>0478 82 43 12</b>	<b>elie.debrauwer@barco.com</b>
Vlaamse kmo? (zie definitie in de handleiding)	<b>Ja/nee (indien nee, aard organisatie toevoegen) Groot bedrijf</b>	
Bereid tot deelname begeleidingsgroep	<b>Ja</b>	<b>Nee</b>
Intentie ondernemingsspecifieke actie	<b>Ja</b>	<b>Nee</b>
<p>Barco doet vandaag al onderzoek naar het gebruik van large language models om haar engineering activiteiten te ondersteunen. Daarnaast heeft het bedrijf enkele use cases in gedachten om llm technologie in te zetten binnen enkele van haar producten.</p> <p>Gezien Barco actief is in o.a. de medische sector, is het bedrijf echter beducht voor mogelijke fouten die de llm zou maken. Veiligheid, betrouwbaarheid en een hoge mate van voorspelbaarheid zijn voor Barco redenen om met de nodige omzichtigheid aan integraties van llms in de eigen producten te beginnen.</p> <p>Door een deelname aan de gebruikersgroep van LISA verwacht Barco versneld zicht te krijgen op hoe om te gaan met de non-deterministische aard van de llms. Ook het uitwisselen van best practices is een reden om tot de gebruikersgroep toe te treden.</p>		

Naam & Handtekening

Datum: **06/06/2024**

Tom Kimpe

VP Technology & Innovation

Barco NV

**Tom Kimpe**  
**(Signature)**

Digitally signed by  
Tom Kimpe (Signature)  
Date: 2024.06.06  
12:01:45 +02'00'

Onderneming	AXI NV	
Beschrijving onderneming en voornaamste activiteiten	<p>AXI is een total solution ICT provider voornamelijk actief in België en Nederland, ontstaan in 1985, locaties in Willebroek (HQ), Gent en Breda en +500 medewerkers. Naast het aanbieden van managed services op infrastructuur ontwikkelt en implementeert AXI haar eigen oplossingen zoals een POS, een dossierbeheer systeem dat wordt ingezet voornamelijk in de publieke sector en een financieel ERP. De producten en services die AXI biedt worden aangevuld met specifieke maatwerk services zoals: applicatie modernisatie op Azure en Oracle, Integraties en analytics &amp; insights.</p>	
Ondernemingsnummer (voor Belgische organisaties) of adres	0407.653.980	
Naam van de contactpersoon en functie	Bjorn Vergaelen – Director Custom Solutions	
Tel en e-mail	+32477292270 bjorn.vergaelen@axi.be	-
Vlaamse kmo? (zie definitie in de handleiding)	Ja/nee (indien nee, aard organisatie toevoegen)	
Bereid tot deelname begeleidingsgroep	Ja	
Intentie ondernemingsspecifieke actie	Ja	Nee
<p>1. Bondige motivatie van de onderneming of non-profitorganisatie tot deelname aan de begeleidingsgroep.</p> <p>Naast het feit dat we vanuit onze eigen producten meer willen inzetten op AI features willen we met onze maatwerk services ons nog explicieter gaan toespitsen op data lifecycle management om uiteindelijk onze klanten te gaan ondersteunen en sturen in hun AI journey.</p> <p>We zijn momenteel onze eerste stappen aan het zetten om AI projecten waarbij regelmatig LLM's worden ingezet met onze bestaande klanten trachten op te starten en ervaren hierin heel wat uitdagingen. Het is vanuit deze optiek dat we graag wensen deel te nemen om ervaringen met sectorenoten te delen.</p> <p>2. De kennissprong die de onderneming verwacht te verwerven dankzij deel A van het COOCK+-project.</p> <p>Inzichten vergaren in de do's en dont's van inzet van LLM's</p>		

3. Toelichting bij de intentie tot het nemen van een ondernemingsspecifieke actie.

De kennis die we hebben vergaard infusen in de lopende projecten

Naam & Handtekening

Datum: 6/6/2024

Bjorn Vergaelen

Director AXI Custom Solutions




Onderneming	Televic Group NV.	
Beschrijving onderneming en voornaamste activiteiten	Kritische communicatie via technologische oplossingen in vier niche markten: treinen, grote vergaderingen, online examensoftware en ziekenhuizen	
Ondernemingsnummer (voor Belgische organisaties) of adres	BE 0402.757.955	
Naam van de contactpersoon en functie	Steven Lauwereins, Research Lead Televic Rail	
Tel en e-mail	0484 757 987	s.lauwereins@televic.com
Vlaamse kmo? (zie definitie in de handleiding)	Nee, grote onderneming NV.	
Bereid tot deelname begeleidingsgroep	Ja	
Intentie ondernemingsspecifieke actie	Ja	
<p>Televic gebruikt vandaag al large language models binnen haar <i>Education</i> producten, en onderzoekt actief hoe het binnen de <i>Rail</i> divisie large language models kan gebruiken om haar bestaande offering robuster te maken. Televic heeft dus al praktische ervaring opgedaan in het veld.</p> <p>Het is net vanuit deze praktische ervaring dat verschillende uitdagingen naar boven komen, zoals:</p> <ul style="list-style-type: none"> <li>- hoe ervoor zorgen dat de output van de llms voldoende correct is?</li> <li>- Hoe omgaan met zeer diverse inputs van gebruikers, die mogelijk de lilm kunnen triggeren in richtingen die niet gewenst zijn (prompt injections).</li> <li>- Hoe bouwen we een validatiesuite die ons toelaat om relatief snel en met voldoende vertrouwen, nieuwe modellen te testen? (belangrijk voor de <i>Rail</i> use-cases, die lokale llms vereisen. De trend lijkt te zijn dat er kleinere modellen – minder paramters - zullen komen, die even krachtig zijn dan hun huidige grotere tegenhangers, en die computationeel minder veeleisend zullen zijn).</li> </ul> <p>Met een deelname aan LISA verwacht Televic ervaringen te kunnen uitwisselen met anderen, en hoopt het bedrijf versneld inzicht te krijgen in best practices, risico's en tooling nodig om op een verantwoorde manier lilm technologie in te zetten. Dit zal toelaten om met meer vertrouwen meerdere use-cases te implementeren.</p>		

Onderneming	Fitme.jobs
Beschrijving onderneming en voornaamste activiteiten	SaaS provider / HR – platform voor het assissen en fitten van mensen en organisaties op basis van soft skills. Sterke focus op evidence based R&D
Ondernemingsnummer (voor Belgische organisaties) of adres	BE0599.835.627
Naam van de contactpersoon en functie	Arend Van Itterbeek, CEO
Tel en e-mail	
Vlaamse kmo? (zie definitie in de handleiding)	Ja
Bereid tot deelname begeleidingsgroep	Ja
Intentie ondernemingsspecifieke actie	Ja
<p>Fitme.jobs is een SaaSplatform dat bedrijven helpt bij het aanwerven van nieuwe medewerkers. Via het platform kunnen de soft skills en competencies van kandidaten getoetst worden aan de noden van de werkgevers.</p> <p>Fitme.jobs werkt op dit moment samen met een aantal (academische) partners rond use cases waarbij deze assessments onder andere via chatbots en natuurlijke taal ondersteund worden. Het bedrijf kijkt daarbij onder andere naar large language model technologie.</p> <p>Tegelijk heeft Fitme.jobs vele vragen rond privacy en confidentialiteit, in combinatie met llms: wat met niet-Europeaanse aanbieders van modellen, zijn open-source modellen capabel genoeg voor de eigen use cases en hoe zetten we dit veilig en robust op?</p> <p>Via een deelname aan de gebruikersgroep hoopt Fitme.jobs ondersteuning te krijgen bij het beslissen hoe het op een veilige manier llms kan inzetten, en hoopt het, samen met de andere leden van de gebruikersgroep, ervaringen uit te wisselen rond do's and don'ts.</p>	

Naam & Handtekening

Datum:

**Arend Van  
Itterbeek  
(Signature)**

**Digitally signed by  
Arend Van Itterbeek  
(Signature)**

Date: 2024.06.06  
16:53:21 +02'00'

Onderneming	Cognit	
Beschrijving onderneming en voornaamste activiteiten	Cognit is een softwarebedrijf dat onder de productnaam Involv een intranetoplossing aanbiedt aan haar klanten, gebaseerd op MS 365.	
Ondernemingsnummer (voor Belgische organisaties) of adres	891 127 518	
Naam van de contactpersoon en functie	Tim Bogemans, Bestuurder	
Tel en e-mail	0494/033660 tim.bogemans@cognit.be	
Vlaamse kmo? (zie definitie in de handleiding)	Ja	
Bereid tot deelname begeleidingsgroep	Ja	Nee
Intentie ondernemingsspecifieke actie	Ja	Nee
<p>Cognit is een softwarebedrijf dat onder de productnaam Involv een intranetoplossing aanbiedt aan haar klanten, gebaseerd op MS 365. Vandaag heeft het bedrijf reeds een beperkte genAI functionaliteit in haar platform (automatische vertalingen), in de komende releases gaat het bedrijf volop inzetten op llm-gebaseerde functionaliteit. Denk aan llm-gebaseerd herschrijven van teksten in een specifieke tone-of-voice, doen van voorstellen voor artikels gebaseerd op korte teksten, genereren van beelden ter ondersteuning van een gegeven artikel. Het bedrijf heeft vandaag al met verschillende klanten/gebruikers gevalideerd dat dit een grote meerwaarde voor hen zou betekenen.</p> <p>Desalniettemin de strategische keuze om volop in te zetten op llm en genAI technologie, leeft bij het bedrijf toch een zekere angst. Het bedrijf heeft al te maken gehad met een geval waarbij de llm-technologie niet-wenselijke content produceerde, wat leidde tot reputatieschade.</p> <p>Cognit is dan ook enthousiast om deel te nemen aan LISA: verwacht wordt dat Cognit vanuit LISA concrete tips, tooling en best practices worden aangericht die het bedrijf kan integreren binnen de eigen software en ter ondersteuning van de eigen software development processen. Het bedrijf is ook geïnteresseerd in hoe het kan meten of de gebruikers de door llms gegenereerde content effectief aansluit bij de verwachtingen.</p>		

Naam & Handtekening

Datum:

07/06/2024

*Tim Bogemans*

Onderneming		
Beschrijving onderneming en voornaamste activiteiten	Youston NV – bedrijf actief in document scanning en archivering	
Ondernemingsnummer (voor Belgische organisaties) of adres	Mondeolaan 1 Genk	
Naam van de contactpersoon en functie	Vanoeveren Wim - CTO	
Tel en e-mail	0486137243	wvanoeveren@iguana-dms.com
Vlaamse kmo? (zie definitie in de handleiding)	Ja/nee (indien nee, aard organisatie toevoegen) ja	
Bereid tot deelname begeleidingsgroep	Ja	Nee
Intentie ondernemingsspecifieke actie	Ja	Nee

Youston is een bedrijf dat actief is in de digitalisering, scanning en archivering van documenten. Het bedrijf heeft door de jaren heen een omvangrijke en zeer gespecialiseerde set OCR tools ontwikkeld. Deze tools zijn in staat om zelfs slecht leesbare documenten toch in te lezen. Het bedrijf experimenteert al even met gebruik van ILM-aangedreven agents. Deze agents laten toe om via prompting op een semi-autonome manier de bovenvermelde toolset te configureren op de wensen van de klant. De eerste bescheiden tests van Youston wezen uit dat dit, mits nog de nodige bijkomende R&D, mogelijk zou kunnen zijn.

Hoewel de concrete use-cases van Youston nog de nodige R&D zullen vragen, wenst het bedrijf toch in te stappen in de gebruikersgroep. Youston verwacht dat het de komende jaren extensief gebruik zal maken van ILM-gebaseerde agents en wil zich vandaag al voorbereiden op de uitdagingen van morgen:

- Hoe test en monitor je de effectiviteit van een ILM-agent gebaseerd systeem?
- Hoe hou je de kosten onder controle, zeker als je weet dat agents function calling kunnen doen, zichzelf meerdere malen kunnen oproepen, etc?
- In welke mate kunnen we snel evalueren of nieuwere, vaak kleinere modellen qua accuraatheid voldoen voor onze use cases (kleinere modellen zijn significant goedkoper).

Youston verwacht dat het de inzichten opgedaan in LISA zal aanwenden om de eigen ILM-agent applicatie robuster te maken.

Naam & Handtekening

Vanoeveren Wim

Datum: 09/08/2024

Onderneming	Metrilio / THE TALENTBOX	
Beschrijving onderneming en voornaamste activiteiten	The Talentbox is de Belgische distributeur van het HR SaaS product Metilio.	
Ondernemingsnummer (voor Belgische organisaties) of adres	BE0878963025	
Naam van de contactpersoon en functie	JAN PETROONS BESTUURDER	
Tel en e-mail	0475 31 76 48	JAN.PETROONS@THETALENTBOX.COM
Vlaamse kmo? (zie definitie in de handleiding)	<input checked="" type="checkbox"/> /nee (indien nee, aard organisatie toevoegen)	
Bereid tot deelname begeleidingsgroep	<input checked="" type="checkbox"/> Ja	Nee
Intentie ondernemingsspecifieke actie	<input checked="" type="checkbox"/> Ja	Nee
<p>Metrilio bouwt innovatieve HR software die bedrijven toelaat hun HR processen te stroomlijnen. Metrilio heeft al verschillende vragen gekregen van klanten om "iets te doen" met generatieve AI en large language models. De mogelijkheden lijken ook legio: vertalingen, chatten met documenten, e.d.</p> <p>Toch houdt Metrilio op dit moment de boot een beetje af: Er zijn ernstige bezwaren rond privacy (verschillende gesprekspartners hebben al aangegeven dat HR-data naar spelers als OpenAI doorsturen, geen optie is), de accuraatheid van (open source) llm modellen en de te verwachten impact op de eigen manier van werken maken dat het team eerst grondig wil evalueren of, en op welke manier, het llms kan inzetten in de eigen applicatie.</p> <p>Met een deelname aan de gebruikersgroep van LISA verwacht Metrilio een aantal antwoorden te krijgen op bovenstaande bezwaren, om zo op een weloverwogen manier de stap te kunnen zetten richting llms.</p>		

Naam & Handtekening

JAN PETROONS



Datum: 7/6/2024

Onderneming	Axiants
Beschrijving onderneming en voornaamste activiteiten	<p>Axiants begeleidt klanten in hun digitale transformatie en ontwerpt, bouwt, implementeert en onderhoudt software en hardware oplossingen op maat van onze klant.</p> <p>Een oplossing kan bestaan uit standaard software, op maat gemaakte software applicaties, SaaS, PaaS, managed services, ...</p> <p>Axiants is een merk van Vinci Energies, is aanwezig in 25 landen en heeft 12.000 medewerker.</p> <p>Axiants is actief in de industrie, healthcare, life sciences, e-learning, banken en verzekeringen en overheid.</p>
Ondernemingsnummer (voor Belgische organisaties) of adres	BE0458581158 Verlorenbroodstraat 122, 9820 Merelbeke
Naam van de contactpersoon en functie	Roel Vermeersch (Business Unit Manager)
Tel en e-mail	0478/324.337   <a href="mailto:Roel.vermeersch@axians.com">Roel.vermeersch@axians.com</a>
Vlaamse kmo? (zie definitie in de handleiding)	Nee (NV en deel van een grote groep)
Bereid tot deelname begeleidingsgroep	Ja
Intentie ondernemingsspecifieke actie	Ja
Axiants is een integrator die actief is in verschillende sectoren. Zo bouwt het bedrijf oplossingen voor onder andere de manufacturing industry en de publieke sector.	
Binnen een aantal use cases ziet Axiants de opportunitet om het ganse interactiemodel tussen gebruiker en computer in vraag te stellen, dankzij spraak- en/of natuurlijke taal-interfaces. Het bedrijf heeft reeds een aantal eerste proof-of-concepts ontwikkeld om ervaring op te doen met large language models, en ervaarde daarbij dat het kostenplaatje van werken met llms lang niet duidelijk en onder controle is. Axiants wil zich ook verdiepen in het lokaal ter beschikking stellen van llms, zonder gebruik te maken van de publieke services zoals OpenAI, en dit zonder de accuraatheid in het gedrang te brengen	
Met haar deelname aan LISA verwacht Axiants beter in kaart te kunnen brengen of de ROI van llm-gebaseerde voor hun use cases goed zit. Ook het a-priori voldoende testen van een llm-applicatie, is iets waar Axiants interesse in heeft.	

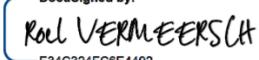
Naam & Handtekening

Roel VERMEERSCH

Business unit Manager

Datum: 7/6/2024

DocuSigned by:

  
E34C324FC6E4492...

Onderneming	King and Queen Journeys	
Beschrijving onderneming en voornaamste activiteiten	<p>King and Queen Journeys biedt teams inzicht, inspiratie en <i>tools</i> om succesvol samen te werken.</p> <p>We brengen het collectieve potentieel naar voren met respect voor elk teamlid.</p> <p>We doen dit vanuit POWER &amp; LOVE, met focus op wat het team samen wil realiseren, in verbinding met elkaar.</p>	
Ondernemingsnummer (voor Belgische organisaties) of adres	BE 0744.564.773	
Naam van de contactpersoon en functie	Hans Keppens, King of Tech	
Tel en e-mail	+32 477 56 41 87	hans.keppens@kingandqueenjourneys.com
Vlaamse kmo? (zie definitie in de handleiding)	Ja	
Bereid tot deelname begeleidingsgroep	Ja	Nee
Intentie ondernemingsspecifieke actie	Ja	Nee
<p>King and Queen Journeys gelooft dat het inzetten van (generatieve) Artificiële Intelligentie kan helpen om bedrijven productiever te maken.</p> <p>King and Queen Journeys ziet echter ook de moeilijkheden, gevaren en/of tekortkomingen, en wil deze beter begrijpen om de kwaliteit van onze begeleiding en van onze producten hoog te houden.</p> <p>We willen graag deelnemen in de begeleidingsgroep, en zullen onze inzichten en use cases delen om het project te helpen slagen.</p> <p>King and Queen Journeys gelooft dat we in de toekomst AI assistenten als deel van het team gaan bekijken, en speelt met het idee om hiervoor eigen producten te ontwikkelen.</p>		

Naam & Handtekening

Datum: 07/07/2024



Hans Keppens

Onderneming	Play it	
Beschrijving onderneming en voornaamste activiteiten	<p>Play it is een jong en ambitieus Saas-bedrijf dat behoort tot de marktleiders in game based learning.</p> <p>Met Play it Safe, Play it Secure en onze Play it Creator bieden we leeroplossingen voor het trainen van (veiligheids)procedures, cyber security en GDPR en het ontwikkelen van custom opleidingen voor elk bedrijf. Standaard of op maat en dat zowel voor middelgrote bedrijven als voor grote namen zoals ABInBev, Coca-Cola, Bayer, Delhaize, Pfizer, Lidl, Borealis en Basic Fit. Met onze simulaties helpen we bedrijven om de kennis en skills van hun medewerkers te verbeteren. En dat allemaal omdat game based learning werkt! Meer informatie op <a href="http://www.playit.training">www.playit.training</a>.</p>	
Ondernemingsnummer (voor Belgische organisaties) of adres	BE0671.574.550	
Naam van de contactpersoon en functie	Lieselotte Verplancke, Head of Delivery	
Tel en e-mail	0472/52.49.48	lieselotte@playit.training
Vlaamse kmo? (zie definitie in de handleiding)	Ja	
Bereid tot deelname begeleidingsgroep	Ja	
Intentie ondernemingsspecifieke actie	Ja	
<p>1. Bondige motivatie van de onderneming of non-profitorganisatie tot deelname aan de begeleidingsgroep.</p> <p>Via verschillende innovatie projecten verkennen we bij Play it vandaag al de opportuniteiten zowel om de huidige workflow (analyse, design, implementatie van games) als de distributie (gepersonaliseerd leren) te verbeteren dankzij (gen)AI. De huidige evolutie en de snelheid van AI is ongezien en daagt ons uit om mee te blijven met de kansen en opportuniteiten die genAI biedt voor ons product en onze markt, en uiteraard ook met de uitdagingen en de risico's die het stelt.</p> <p>2. De kennissprong die de onderneming verwacht te verwerven dankzij deel A van het COOCK+-project.</p>		

Onze AI-innovatieroadmap loopt nog wel even door (al minstens tot 2028). Onderweg zullen we ongetwijfeld geconfronteerd worden met reeds gekende maar ook nieuwe uitdagingen op vlak van robuustheid, cyberveiligheid, performantie, kostoverwegingen, regelgeving en de integratie. Vandaag gaat dat bv. over ethiek en privacy (welke user data kan worden gebruikt en hoe), over competenties (wat moet een team anders kunnen dan vroeger, welke impact op HR en processen), over weerstand bij klanten jegens het gebruik van LLMs, etc.), over het maken van de beste keuzes of combinaties van AI toepassingen, etc. Dankzij deelname aan de begeleidingsgroep blijven we up-to-date en kunnen we tegelijk goede praktijken uitwisselen van alle parallelle initiatieven.

3. Toelichting bij de intentie tot het nemen van een ondernemingsspecifieke actie.

Afhankelijk van de projectresultaten is Play it bereid om de mogelijkheden en toegevoegde waarde van advies, exploratie of enige andere OSA te bekijken.

Naam & Handtekening

Lieselotte Verplancke

Datum: 07/06/2024

Onderneming	UpdatePro	
Beschrijving onderneming en voornaamste activiteiten	Digitaal uitzendkantoor zonder werving & selectie.	
Ondernemingsnummer (voor Belgische organisaties) of adres	BE0450.903.114	
Naam van de contactpersoon en functie	Vincent Willems – Product manager	
Tel en e-mail	<a href="mailto:vincent@update-pro.be">vincent@update-pro.be</a>	+32 471 69 68 35
Vlaamse kmo? (zie definitie in de handleiding)	Ja/nee (indien nee, aard organisatie toevoegen)	
Bereid tot deelname begeleidingsgroep	Ja	Nee
Intentie ondernemingsspecifieke actie	Ja	Nee

UpdatePro is een payroll-kantoor voor tijdelijke werknemers. Het bedrijf hanteert vandaag reeds een digitale aanpak om haar eigen werking te ondersteunen, en is volop bezig met de achterliggende software en loonmotor als een eigen softwareproduct in de markt te zetten.

Het bedrijf heeft reeds geëxperimenteerd met large language models om bijvoorbeeld op basis van wetteksten en CAO's adviezen te geven. Daaruit leerde het bedrijf dat deze use case, mits voldoende bewaking van de correctheid en robustheid van de llms-outputs, een significante meerwaarde kan betekenen voor haar eindgebruikers.

UpdatePro blijft het wel een uitdaging vinden om de correctheid van de outputs te garanderen, en stelt zich ook de vraag hoe feedback op het gebruik van de llms te capteren om desgewenst bij te sturen. Ook het luik validatie, zowel tijdens development als in productie, zijn nog open vragen.

Met een deelname aan de gebruikersgroep van LISA verwacht UpdatePro inzichten te krijgen in hoe op een correcte, veilige en robuste manier llms te integreren. Ook inzichten van peers en tips hoe llms-apps te testen, zijn redenen om de gebruikersgroep te vervroegen.

Naam & Handtekening

Vincent Willems 10/06/2024



Datum:

## DEEL 2: PROJECTBESCHRIJVING

### 1. Doelstellingen

#### Context

De opkomst van Artificiële Intelligentie—en specifiek *generatieve AI* (genAI)—is bezig met onze samenleving ingrijpend te veranderen. Deze technologieën stimuleren innovaties over diverse sectoren heen. De schijnbaar exponentiële groei van AI-toepassingen bewijst dat we onomkeerbaar op weg zijn naar een toekomst waarin AI onmisbaar is. Ook bedrijven moeten zich aanpassen om competitief te blijven in deze snel-evoluerende markt.

In de voorhoede van nieuwe AI-toepassingen, vinden we zogenaamde *Large Language Models* (LLM's). Deze systemen kunnen natuurlijke taal begrijpen en genereren, wat ze uiterst waardevol maakt voor diverse zakelijke toepassingen waaronder klantenservice, contentcreatie en data-analyse. Bedrijven zien de vele voordelen van LLM's (o.a. verbeterde efficientie en kostenbesparing), waardoor LLM's snel in populariteit winnen. Aan de hand van LLM's willen bedrijven hun klanten een gepersonaliseerde ervaring aanbieden en zo hun concurrentiepositie versterken.

Toch verschillen LLM's aanzienlijk van traditionele software, wat vaak tot onduidelijkheden leidt bij de integratie met bestaande systemen. Bovendien kunnen de lange trainings- en fine-tuningprocessen van LLM's het ontwikkelingsproces verlengen. De integratie van LLM-technologieën in softwareproducten heeft dus een aanzienlijke impact op de development practices. Zo moeten ontwikkelteams rekening houden met de inherente variabiliteit en het niet-deterministische gedrag van LLM's, wat problemen kan opleveren bij het ontwikkelen van uitgebreide testcases om de output van de LLM te valideren. Regressietesten worden heel belangrijk omwille van de snelle evolutie in het domein van LLM's waarbij continu nieuwe, efficiëntere modellen beschikbaar komen. De regressietesten stellen ontwikkelaars in staat om snel en betrouwbaar nieuwe modellen te evalueren en te integreren zonder dat dit ten koste gaat van de kwaliteit of prestaties van het product. Toch blijft het testen van LLM's niet evident aangezien LLM's typisch gebruikt worden om met gebruikers te interageren, waarbij naast het onvoorspelbare gedrag van het LLM-model ook nog eens het onvoorspelbare gedrag van de gebruiker bijkomt. Geautomatiseerde testsuites kunnen hierbij helpen door een breed scala aan scenario's te simuleren en te analyseren. Verder kan het valideren van de performantie van het model worden ondersteund door het gebruik van specifieke evaluatiemetrieken die relevant zijn voor de beoogde usecases.

Daarnaast zijn er ook specifieke problemen die eigen zijn aan het gebruik van LLM's. Zo kunnen LLM's *hallucineren*, waarbij ze onjuiste of verzonnen informatie genereren, waardoor de uitvoer van het systeem onnauwkeurig wordt. Daarnaast kan de uitvoering van een LLM onverwacht hoge kosten met zich meebrengen. Deze kosten kunnen een uitdaging zijn voor organisaties met beperkte middelen.

Als laatste brengen LLM's ook verschillende (nieuwe) beveiligingsproblemen met zich mee. Kwaadwillenden kunnen proberen de uitvoer van de LLM te manipuleren door misleidende instructies in te voegen. Aanvallers kunnen ook het model proberen te stelen om het dan te repliceren. Dit kan leiden tot het verlies van intellectual property. Daarnaast kunnen LLM's gevoelige data bevatten, die gelekt kan worden als ze niet adequaat beschermd wordt. Dit kan bepaalde juridische risico's met zich meebrengen.

#### Concrete Doelen

Sirris en DistriNet willen in dit project samenwerken met als doel de LLM-technologie sneller inzetbaar te maken voor Vlaamse softwareontwikkelaars. De aanleiding voor dit project ontstond onder andere uit individuele interacties met digitale productenbouwers, die deze specifieke behoeften op dit gebied aankaartten. Ze zien mooie toepassingen van LLM's in hun producten, maar hebben te weinig expertise om die technologie op een effectieve, efficiënte en veilige manier in hun digitaal platform te integreren. In de eerste plaats zal dit project dan ook de kennis rond LLM's bij Vlaamse bedrijven vergroten.

Concreet is het project in vier stukken opgedeeld, die elk specifieke onderwerpen bespreken. Het eerste deel is gerelateerd aan de implementatie van LLM's in nieuwe usecases. Aangezien LLM's een relatief nieuwe technologie zijn, hebben veel ontwikkelaars nog weinig of geen ervaring met deze systemen. Het onvoorspelbare karakter van LLM's, wat voortkomt uit de nieuwe AI-gedreven werkwijze om met gebruikersinvoer en data om te gaan, zorgt ervoor dat gevestigde data en toepassingsarchitecturen, alsook de ontwikkelprocessen herbekijken moeten worden. De volgende onderwerpen worden behandeld:

- Opdrijven van kennis en expertise: Veel bedrijven hebben niet voldoende kennis en expertise in huis op het gebied van AI en specifiek LLM's. Het integreren van LLM's als een fundamenteel aspect van een applicatie vereist vaak een diepgaand begrip van de werking van dergelijke systemen.
- Evaluatie van methodologieën en tools: Het hele landschap van generatieve AI is volop in verandering. Het is dan ook niet verwonderlijk dat er veel verschillende tools en frameworks zijn die dergelijke technologieën ondersteunen, met elk hun specifieke voor- en nadelen. Het begrijpen van de trade-offs tussen verschillende tools en technologieën is een uitdaging voor bedrijven.
- Technologiewacht: Nieuwe technologieën, frameworks en best practices worden regelmatig geïntroduceerd. Hierdoor is het belangrijk om een proactieve technologiewacht te hebben, waarin bedrijven continue op de hoogte worden gebracht van de nieuwste ontwikkelingen op het gebied van modellen, tools, libraries en het ecosysteem als geheel.
- Vendor lock-in vermijden: Het trainen en exploiteren van een LLM-basismodel is een zeer kostelijke zaak. Momenteel zijn er slechts een beperkt aantal grotere partijen die dergelijke modellen gecommercialiseerd hebben, waar andere (Vlaamse) bedrijven dan gebruik van kunnen maken door hun bedrijfseigen data te integreren met het aangeboden basismodel. Gezien de beperkte hoeveelheid aanbieders, lopen bedrijven echter het risico op vendor lock-in. Bedrijven moeten zich hier in de eerste plaats van bewust zijn, en kunnen technieken toepassen om de afhankelijkheid van een provider te vermijden.

Het tweede deel draait rond de potentiële veiligheidsproblemen die gelinkt zijn met het gebruik van deze nieuwe technologie. Bedrijven worden bewust gemaakt van de beveiligingsaspecten in het ontwerp en worden geholpen bij het implementeren van veilige ontwerprincipes. Uiteindelijk zullen ze in staat zijn om zelfstandig potentiële veiligheidsproblemen te identificeren en oplossingen te vinden die passen binnen hun bredere ontwikkelingsvereisten. De volgende onderwerpen worden behandeld:

- Onbedoeld delen van gevoelige informatie: LLM-gebaseerde systemen kunnen gemanipuleerd worden om geheimen en vertrouwelijke bedrijfsgegevens te delen die diep in het LLM-model verborgen zitten.
- Manipulatie van invoer: Aanvallers kunnen de invoer van het systeem op verschillende beïnvloeden en daardoor de beperkingen opgelegd aan het systeem omzeilen.

- **Modeldiefstal:** *Onbevoegde toegang tot en data-extractie uit LLM-modellen kan leiden tot economisch verlies en reputatieschade. Het kan een aanvaller ook een concurrentievoordeel geven omdat die het gestolen model kan gebruiken zonder in een eigen model te moeten investeren.*
- **Beschikbaarheid van het systeem:** *Aanvallers kunnen het systeem manipuleren zodat het meer processorkracht vraagt dan normaal het geval is. Zo kunnen ze het systeem onbeschikbaar maken voor andere gebruikers.*

Het derde deel richt zich op de uitrol en werking van de LLM, het onderhoud, en de impact op de CI/CD pipeline. De best practices van DevOps worden vertaald naar de context van LLM-systemen, waarbij ingezet wordt op automatisering zodat de ontwikkeling, implementatie en onderhoud van deze systemen geoptimaliseerd wordt. De volgende onderwerpen worden behandeld:

- **Integratie van LLM's in DevOps-pipelines:** *De best practices van DevOps worden vertaald naar de context van LLM-systemen, waarbij ingezet wordt op automatisering zodat de ontwikkeling, implementatie en onderhoud van deze systemen geoptimaliseerd wordt.*
- **Kostenaspect:** *Voor bedrijven is het belangrijk om correct de kosten van een LLM-systeem te kunnen inschatten. Dit omvat zowel de initiële kosten voor de ontwikkeling en integratie van de modellen als de operationele kosten voor het gebruik en onderhoud ervan.*
- **Operationele aspecten:** *Ook operationele aspecten komen aan bod, waarbij gestreefd wordt naar een evenwicht tussen prestaties en betrouwbaarheid. Dit omvat onder meer het opzetten van effectieve monitoring om de prestaties en het gedrag van het systeem te kunnen volgen en analyseren.*
- **Functionele testen:** *LLM's werken anders dan reguliere software. In hun werking zit een inherente vorm van onzekerheid en niet-determinisme ingebouwd, die enerzijds zorgt voor creativiteit bij het genereren van tekst, maar anderzijds er ook voor zorgt dat de uitvoer van een LLM bij elke aanvraag anders is. Het (geautomatiseerd) testproces voor LLM's moet hier bijgevolg ook rekening mee houden en zal anders werken dan bij andere software.*

Tot slot richt het vierde en laatste deel zich op de complexe juridische implicaties van het gebruik van LLM's. Er wordt meerbepaald gekeken naar de juridische aansprakelijkheid die een bedrijf heeft, wanneer het een LLM-systeem gebruikt. De volgende onderwerpen worden behandeld:

- **De Europese AI act:** *Binnenkort wordt de Europese AI act van kracht, wat implicaties heeft voor bedrijven die gebruik maken van LLM's. Er wordt een overzicht gegeven van de nieuwe regelgeving.*
- **Privacy en gegevensbescherming:** *Het gebruik van LLM's kan leiden tot het verzamelen en verwerken van grote hoeveelheden gegevens, waaronder mogelijk persoonlijke informatie. Daarom kunnen applicaties onder de jurisdictie van de Algemene Verordening Gegevensbescherming (AVG, Eng.: GDPR) vallen.*
- **Aansprakelijkheid in combinatie met LLM's:** *De vraag naar wie er verantwoordelijk is in het geval van fouten of schade veroorzaakt door een LLM-systeem, en of dit verzekeraar is, is een belangrijk juridisch aspect dat moet worden overwogen. Dit kan onder meer betrekking hebben op contractuele aansprakelijkheid, productaansprakelijkheid en professionele aansprakelijkheid.*

- *Auteursrechten: Bij het trainen van een LLM worden grote hoeveelheden gegevens gebruikt, en het is vaak onduidelijk welke specifieke datasets precies zijn gebruikt. Hierdoor kunnen auteursrechten mogelijk worden geschonden, met juridische geschillen tot gevolg.*

In de vier delen van het project wordt de kennis bij de deelnemende bedrijven structureel opgebouwd, rekening houdend met hun specifieke noden. Deze opbouw zorgt ervoor dat elk bedrijf de benodigde inzichten en vaardigheden opdoet om effectief gebruik te maken van LLM-technologieën. Naast de directe kennisoverdracht naar de deelnemende bedrijven, willen we ervoor zorgen dat deze kennis niet verloren gaat na het einde van het project. Daarom richten we ons ook op andere bedrijven in de bredere Vlaamse context die (eventueel pas na het einde van deel 1 van het project) met LLM's aan de slag willen gaan. Dit doen we door te investeren in het opzetten van een kenniscentrum rond het gebruik van LLM-technologie, dat we ook lang na het project zullen onderhouden. Dit kenniscentrum zal dienen als verzamelplaats voor al het gegenereerde materiaal tijdens de looptijd van het project, zodat zowel bedrijven in de begeleidingsgroep als daarbuiten dit kunnen gebruiken als naslagwerk. Op deze manier waarborgen we dat de opgedane kennis breed beschikbaar blijft en bijdraagt aan de verdere ontwikkeling en toepassing van LLM-technologie in Vlaanderen.

Een gedetailleerd overzicht van de technische onderwerpen die behandeld zullen worden in het LISA-project, volgt in Sectie 3: Werkplan.

### **Bedrijfsevolutie doorheen het project en KPI's**

De kennisopbouw en -overdracht is een groeiproces voor de bedrijven in de doelgroep. Het beoogde resultaat is een versnelling van de adoptie van LLM-technologieën in Vlaanderen. Dit wordt bereikt door de doelgroep in staat te stellen vijf stadia te doorlopen, waarbij elk bedrijf kan instappen op het niveau dat voor hen relevant is. De verschillende stadia die doorlopen (en bereikt) worden, zijn:

1. *Bewustzijn vergroten: Het vergroten van bewustzijn door inzicht te creëren in de vereisten en behoeften van LLM's, met een focus op concrete implementatiemoeilijkheden van dergelijke technologieën.*
2. *Fundamentele kennis verwerven: Kennis van relevante LLM-technologieën verwerven, zowel op het gebied van implementatie, deployment, als veiligheid.*
3. *Diepgaande kennis verwerven: Kennis rond state-of-the-art LLM-technologieën verwerven en deze integreren tot een veilige end-to-end oplossing met aandacht voor voor- en nadelen en andere afwegingen.*
4. *Concrete aanpak ontwikkelen: Een aanpak voor het gebruik van LLM's opstellen en een integratieplan creëren, gebaseerd op de inzichten uit punten 1, 2 en 3.*
5. *Implementeren en integreren: Implementatie van een veilige LLM-integratie en een effectieve uitrol (inclusief het gebruik van tools om de uitgerolde LLM te monitoren).*

Niet elk bedrijf zal instappen met dezelfde kennis. Sommige bedrijven hebben al geëxperimenteerd met LLM's en hebben al basiskennis vergaard. Andere bedrijven zijn geïnteresseerd in het gebruik van LLM's, maar hebben nog geen voorkennis. Door de getrapte aanpak van het project is dit echter geen probleem: bedrijven zonder voorkennis worden eerst naar het niveau getild van bedrijven die al enige voorkennis hebben. Daarna wordt die kennis verder verdiept, met een implementatiecase als uiteindelijk doel.

De succesindicatoren van deze doelen van het project worden gemeten via de volgende KPI's:

- **KPI 1:** *het cumulatief aantal punten voor de collectieve acties gelinkt aan deel A van het COOCK-project en uitgevoerd voor het einde van deel A: 30, 66+*
- **KPI 2:** *aantal unieke ondernemingen die minstens 1 ondernemingsspecifieke actie opstarten, gelinkt aan deel A van het COOCK-project, tijdens of tot twee jaar na het einde van deel A: 0, 6, 12, 14+*
- **KPI 3:** *het cumulatief aantal punten voor de opgestarte ondernemingsspecifieke acties, tijdens of tot twee jaar na het einde van deel A: 0, 40, 60, 66, 66+*

Deze waardes van deze KPI's over de jaren heen reflecteren de structuur van het project. Het eerste jaar zal gericht zijn op kennisoverdracht en het harmoniseren van kennis binnen de bedrijven. Vervolgens zal het tweede jaar zich richten op de daadwerkelijke uitrol van de nieuwe technologieën binnen de bedrijven.

## 2. Fit in het programma

### Projectpartners

Dit project wordt uitgevoerd in een samenwerkingsverband tussen Sirris en DistriNet.

Sirris is de vertrouwenspartner van alle Belgische bedrijven met een honger naar technologische innovatie. Eenvoudig gesteld helpt Sirris bedrijven hun innovatieambities waar te maken met hands-on ondersteuning.

Sirris heeft veel ervaring met het begeleiden van bedrijven op vlak van innovatie en het opzetten van partnerschappen (meer dan 1300 innovatieprojecten per jaar) en met het bouwen van proof of concepts en demonstratoren. Het zal deze ervaring inbrengen in dit COOCK+ project.

Artificiële Intelligentie staat op de Sirris-agenda sinds 2009, toen de eerste data-innovatieprojecten van start gingen. Vandaag heeft Sirris een industriële portefeuille van ongeveer 50 algemene AI-projecten gerealiseerd, waarbij ongeveer een 100tal lead user bedrijven bij betrokken zijn.

Een kleine selectie van een aantal lopende en afgelopen AI-initiatieven waar Sirris bij betrokken is:

- **SAMUEL** (april 2019 - november 2022) is een ITEA-project over slimme additieve productie. (<https://itea4.org/project/samuel.html>)
- **DREDGE** (mei 2019 - april 2022) is een O&O-project ondersteund door VLAIO met als doel het onderzoeken en valideren van efficiënte oplossingen voor data-infrastructuur, technologieën en methodologieën die het efficiënt verzamelen, opslaan en overdragen van gebruiksgegevens van veiligheidskritische producten.
- **BitWind** (oktober 2018 - december 2021) is een project ondersteund door de FOD Economie, K.M.O., Middenstand en Energie dat zich richt op de ontwikkeling van nieuwe kunstmatige intelligentietechnieken op data van operationele offshore windparken.
- **AI4DETAIL** (april 2020 - maart 2023) is een COOCK-project dat werd ondersteund door VLAIO. Vandaag de dag worden producten meestal ontworpen, ontwikkeld en onderhouden zonder gedetailleerde kennis over wie ze gebruikt, voor welke doeleinden en onder welke omstandigheden. Digitalisering biedt een kans om dit te verbeteren, door continu op grote schaal gegevens te verzamelen over hoe deze producten in het veld worden gebruikt en door deze gegevens te exploiteren via AI- en ML-technieken.

- **ARIAC** (januari 2021 - december 2026) is een project van het TRAIL Institute initiative in het kader van het plan DigitalWallonia4.ai van het Waals Gewest. Het project heeft als doel het onderzoek op het gebied van AI in Wallonië te versterken door nieuwe technologische tools te ontwikkelen en te valideren op basis van kunstmatige intelligentietechnieken en deze kn
- - **C-DATA** (september 2022 - augustus 2025) is een VLAIO ICON O&O project met als doel de basis te leggen voor de digitalisering, automatisering en optimalisering van het volledige additive manufacturing (AM) proces.
- **Sustain.brussels** ([https://www.sustain.brussels/nl\\_BE](https://www.sustain.brussels/nl_BE)). Sirris is coordinator van deze Europese digitale innovatiehub

DistriNet is een onderzoeksgruppe van het departement Computerwetenschappen van de KU Leuven. Het onderzoek focust zich op gedistribueerde en veilige software. DistriNet heeft een traditie van vraaggedreven onderzoek in nauwe samenwerking met industriële partners en is momenteel actief in een 30-tal nationale en internationale projecten, gaande van fundamenteel onderzoek tot toegepast onderzoek. De onderzoeksexpertise van DistriNet beslaat onder andere de combinatie van LLM's en andere AI-technologieën met beveiliging (zowel het gebruik van AI in beveiligingstoepassingen, als de veiligheid van AI-systeem).

Een kleine selectie van een aantal AI-gerelateerde projecten waar DistriNet bij betrokken is en een kleine selectie van recente publicaties rond beveiliging van/met AI:

- **CSAI** (maart 2021 – september 2023) is een ICON-project dat AI voor cybersecurity verbetert door adaptieve en zelflerende systemen te ontwikkelen. DistriNet onderzoekt de robuustheid van machine learning in beveiligingsanalyses. De kennis wordt toegepast in vier industriële gevallen, resulterend in geavanceerde beveiligingstools.
- **KINAITICS** (oktober 2022 – september 2025) is een Horizon Europe project dat AI-gerelateerde cyberfysieke veiligheidsrisico's onderzoekt en innovatieve verdedigingsstrategieën ontwikkelt. Het project richt zich op het ontwerpen van een geïntegreerd kader voor juridische, ethische en technische vereisten, het ontwikkelen van geavanceerde aanvalsframeworks, en het verbeteren van simulators voor nauwkeurige training in realistische contexten.
- **AIDE** (december 2023 – oktober 2026) is een BELSPO-project dat een gefedereerd machine learning-platform definieert en implementeert om de effectiviteit te demonstreren via casestudies. Gefedereerd leren stelt meerdere clients in staat om gezamenlijk een model te trainen zonder gevoelige data te delen. Het project begint met toepassingen in cybersecurity en IoT, gericht op respectievelijk het delen van dreigingsinformatie en voorspellend onderhoud.
- Preuveneers, D., & Joosen, W. (2024). **An Ontology-Based Cybersecurity Framework for AI-Enabled Systems and Applications**. Future Internet, 16(3), 69.
- Meszaros, J., Preuveneers, D., Marquet, E., Peter, I. E., Santos, I. R., Vranckaert, K., ... & Menéndez, N. (2023). **Chatgpt: How Many Data Protection Principles Do You Comply with?**. Available at SSRN 4647569.
- Verheyen, W., Van Hamme, T., Joos, S., Preuveneers, D., & Joosen, W. (2023, August). **Beware the Doppelgänger: Attacks against Adaptive Thresholds in Facial Recognition Systems**. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-11).

- Verdonck, J., De Boeck, K., Willocx, M., Lapon, J., & Naessens, V. (2023, August). *A hybrid anonymization pipeline to improve the privacy-utility balance in sensitive datasets for ML purposes*. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-11).
- Van Hamme, T., Garofalo, G., Preuveneers, D., & Joosen, W. (2023, July). *Masterkey attacks against free-text keystroke dynamics and security implications of demographic factors*. In 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P) (pp. 278-291). IEEE.
- Hernández-Castro, C. J., Liu, Z., Serban, A., Tsingenopoulos, I., & Joosen, W. (2022). *Adversarial machine learning*. In Security and Artificial Intelligence: A Crossdisciplinary Approach (pp. 287-312). Cham: Springer International Publishing.
- Argones Rúa, E., Van Hamme, T., Preuveneers, D., & Joosen, W. (2022). *Discriminative training of spiking neural networks organised in columns for stream-based biometric authentication*. *Int Biometrics*, 11(5), 485-497.

## Doelgroep

De doelgroep van het project bestaat in de eerste plaats uit Vlaamse softwareontwikkelaars. Deze ontwikkelaars bouwen digitale producten en willen LLM's in hun software integreren om nieuwe innovatieve toepassingen te realiseren. De bedrijven in de begeleidingsgroep hebben vaak al concrete ideeën over hoe ze LLM's kunnen inzetten in nieuwe scenario's, waardoor de projectleden in feite *early adopters* zijn van LLM-technologie. Deze bedrijven lopen dus voorop in de exploratie en toepassing van deze geavanceerde AI-modellen. Ze weten echter vaak niet hoe ze er concreet aan moeten beginnen, of wat de potentiële valkuilen zijn bij het gebruik van LLM's (zowel op vlak van DevOps, beveiliging, als juridisch).

We verwachten echter dat LLM-technologie zich verder zal verspreiden en in de toekomst een integraal onderdeel zal worden van uiteenlopende sectoren en toepassingen. Daarom is de doelgroep van het project op lange termijn breder dan enkel de huidige early adopters. Het project richt zich uiteindelijk op een bredere groep bedrijven en ontwikkelaars die in de toekomst willen profiteren van de mogelijkheden die LLM's bieden. Dit betekent dat de kennis en inzichten die binnen het project worden ontwikkeld, niet alleen de huidige deelnemers ten goede zullen komen, maar ook een basis zullen vormen voor een bredere acceptatie en implementatie van LLM-technologie in Vlaanderen.

## Meerwaarde t.o.v. huidige kennis

Het project richt zich op het ondersteunen van (kleine/middelgrote) Vlaamse softwareontwikkelaars bij het integreren van LLM-gebaseerde aspecten in hun digitale producten. Door de innovatieve aard van de technologie, ontbreekt momenteel de kennis grotendeels om dergelijke integraties op een efficiënte en kosteffectieve manier in het softwareontwikkelingsproces te integreren. Dit project realiseert een meerwaarde door de ontbrekende kennis bij de doelgroep op te bouwen. Specifiek wordt dit gekenmerkt door:

- *Het verbreden van de kennis van:*
  - *Algemene implementatie- en integratiemoeilijkheden met LLM's*
    - *Integratie van LLM's in bestaande ontwikkelingsprocessen*
    - *Veiligheid van LLM's*

- *Testen en opvolgen van LLM-implementaties*
  - *Juridische verantwoordelijkheden*
- *Trade-offs en andere afwegingen die een impact hebben op de selectie van state-of-the-art en state-of-practice technologieën*
- *De opbouw van know-how om de kennis toe te passen in concrete cases:*
  - *Het kunnen definiëren van een concrete implementatiestrategie, inclusief de uitrol van een case bij een onderneming (o.a. aan de hand van blueprints die uitgewerkt worden in dit project)*
  - *De case succesvol integreren in de bestaande DevOps-pipeline*

Door deze kennisopbouw en -vertaling zal de go-to-market van bedrijven in onze doelgroep aanzienlijk versneld worden. Enerzijds zullen de resultaten van het project helpen om technische obstakels te overkomen bij de integratie van LLM-oplossingen. Anderzijds zullen de specifieke demonstratoren en trade-off analyses binnen het project bijdragen aan een snellere ontwikkeling van veilige oplossingen. Door vroeg te investeren in AI-verrijkte gebruikersscenario's krijgen de bedrijven in de begeleidingsgroep een aanzienlijk concurrentievoordeel, wat zal leiden tot betere competitiviteit en een sterkere internationale positie.

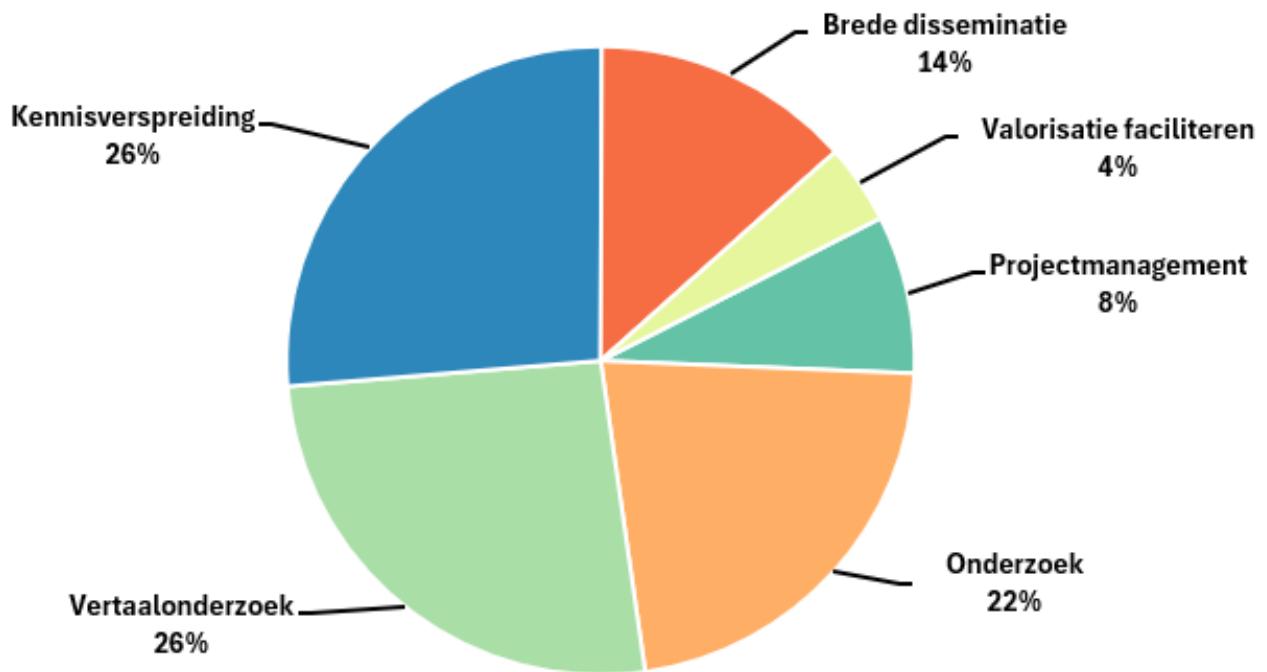
### **Overzicht van de projectaspecten**

Het project bestaat uit vier verschillende delen die elk een specifieke focus hebben. Het werkplan van het project (zie Sectie 3) is echter ingedeeld in werkpakketten volgens de verschillende projectaspecten (onderzoek, vertaalonderzoek, kennisoverdracht, ...). Elk van de vier projectdelen komen dus terug in elk werkpakket.

Het project bestaat uit de volgende projectaspecten (en dus ook overeenkomstige werkpakketten):

0. **Projectmanagement:** *Het opvolgen en sturen van het project om tijdige oplevering van deliverables te garanderen, met aandacht voor rapportering, communicatie met de begeleidingsgroep en implementaties in deel B van het project.*
1. **Kennisopbouw en -vergaring:** *Kennis over LLM's, technologische aanpakken en tools voor het veilig implementeren en testen van LLM-applicaties wordt verankerd. Bovendien worden de juridische vereisten voor het gebruik van AI-technologie gedocumenteerd.*
2. **Vertaling van kennis naar industrie-gedreven usecases:** *Er worden architecturale varianten gedefinieerd die als basis dienen om trade-offs te analyseren m.b.t. de implementatie van een veilige LLM-integratie.*
3. **Kennisoverdracht:** *Er worden interactieve seminars, workshops en demonstraties georganiseerd waarin de begeleidingsgroep samenkomt om state-of-the-art technologieën, best practices en ervaringen met LLM's te bespreken.*
4. **Brede disseminatie:** *De gecreëerde kennis en projectresultaten worden verspreid naar een breder publiek via verschillende kanalen, zoals portals, websites, publicaties, demonstraties en workshops.*
5. **Faciliteren van valorisatie:** *De beschikbaarheid en relevantie van de kennis wordt gegarandeerd door het opzetten van een kennisbank die langdurig beschikbaar blijft en waarbij doorheen het project de veranderingen in het LLM-ecosysteem in kaart gebracht worden en geïntegreerd.*

Onderstaande grafiek geeft een overzicht van de grootte van elk projectaspect, in relatie tot het volledige project:



De aspecten *onderzoek*, *vertaalonderzoek* en *kennisverspreiding* krijgen elk ongeveer een vierde van het budget toegewezen. Het resterende budget wordt, naast het budget voor projectmanagement, gebruikt om de resultaten te verspreiden en te valoriseren naar bedrijven buiten de begeleidingsgroep en naar de toekomst toe.

### 3. Werkplan

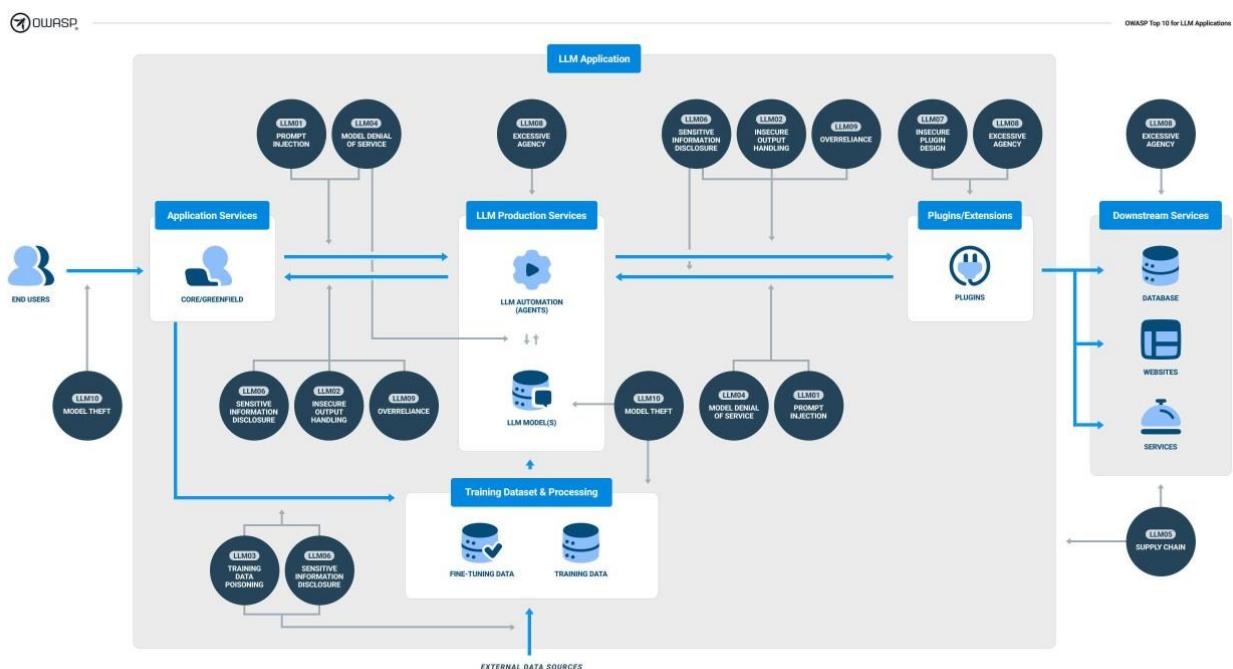
Voor de technische invulling van de werkpakketten, vertrekken we van de concrete noden binnen het Vlaamse landschap van softwarebouwers. Veel bedrijven willen LLM-gebaseerde features uitbouwen en denken eraan, of zijn bezig met, het evalueren van software-architecturen om bepaalde types van usecases te ondersteunen. Het is echter niet altijd duidelijk hoe en waar ze hun softwareprocessen daarvoor moeten aanpassen. Dit is voor velen een urgent probleem en er is een duidelijke vraag om hiermee zeer snel aan de slag te gaan. Op basis van de intakegesprekken, zien we een convergentie naar vier categorieën van usecases voor LLM-gebaseerde functionaliteit (waarbij usecases 1, 2 en 3 de meest voorkomende zijn):

1. **LLM's ter vervanging van 'klassieke' NLP:** Denk hierbij aan het parsen van documenten, entity extraction, sentiment analyse, ...
2. **Chat with the docs:** LLM-technologie wordt gebruikt om in natuurlijke taal te zoeken/interageren met een bestaande kennisdatabank (bv. data opgeslagen in een document/content management systeem)
3. **Ondersteuning bij content creatie:** LLM-technologie wordt aangewend om functionaliteit in het product te bouwen om de gebruiker te helpen met het maken en/of verbeteren van nieuwe content

(bv. het vertalen van artikels, voorstellen doen voor tekst op basis van sleutelwoorden, herschrijven van inhoud in een andere tone-of-voice)

4. **Prompt-based configuration:** Veel software bevat complexe configuratiemogelijkheden (bv. software die custom workflows toelaat). Vaak is het configureren iets moeilijks: je moet enerzijds het domein van de klant goed begrijpen, en anderzijds de mogelijkheden van de software zelf. De configuratie gebeurt dan door wizards en/of no/low code-oplossingen. Via prompt based configuration wordt nu getracht de gebruiker een natuurlijke taalinterface te geven waarin de configuratie wordt beschreven, terwijl achter de schermen LLM's, aan de hand van function calling en/of een agent framework, de workflow opzetten.

Er is een high-level consensus hoe de architectuur van een LLM-applicatie eruit kan zien. Figuur 1 toont [een voorbeeld](#) van een referentie-architectuur van LLM-componenten, maar er zijn [verschillende alternatieven](#) (met elk voor- en nadelen) mogelijk.



Figuur 1: Een voorbeeld van een softwareontwerp voor een LLM-component binnen een applicatie.

Voor elke architectuurcomponent (vectordatabase, embeddings, llmcache, orchestratie, ...), moeten er keuzes gemaakt worden voor welke opkomende technologische bouwblokken gebruikt worden (picone, chromadb, pgvector, openAI, huggingface, gptcache, langchain, ...). Deze bouwblokken zijn beschikbaar zowel in open source als proprietary vorm, maar het is niet zomaar kiezen en toepassen. Dit is een zeer snel evoluerend en rijkgevuld domein. Om de adoptie te versnellen mist er kennis en ervaring bij de doelgroep om de vertaalslag te maken naar technologie die in productie bruikbaar is voor de usecases.

Binnen de Vlaamse softwarebouwers leeft nog veel onzekerheid over hoe ze hun eigen usecases op een veilige, robuuste, betrouwbare en kostefficiënte manier kunnen implementeren. Velen vragen zich daarbij af hoe ze hun huidige manier van werken (bv. requirement engineering, testing, appsec, ...) zullen moeten aanpassen aan het feit dat LLM's, omwille van hun inderterminisme en enorme input- en outputruimte, afwijken van hoe traditioneel naar een softwaresysteem wordt gekeken.

Enkele concrete voorbeelden van uitdagingen:

- *Hoe kunnen we een voldoende correcte en gepaste output garanderen?*
- *We zien de waarde wel van een LLM-gebaseerde feature, maar kunnen de kost, en dus de ROI, niet goed inschatten.*
- *Hoe kunnen we ons beveiligen tegen zaken zoals prompt injection?*
- *Hoe kunnen we snel evalueren of nieuwere, kleinere modellen ook volstaan voor onze usecase?*
- *Hoe moeten we omgaan met requirements rond privacy en confidentialiteit*

Het LISA-project bestaat uit vier verschillende delen die elk een specifieke focus hebben. Gebaseerd op de input van de doelgroep, geven we elk van die delen een invulling die de vastgestelde noden afdekt.

In het eerste deel ligt de focus op het correct implementeren en integreren van LLM-oplossingen. Om LLM's te gebruiken binnen een specifieke bedrijfscontext vereist die gespecialiseerde kennis van deze context. Wanneer deze kennis niet aanwezig is loopt men het risico op onvolledige of zelfs volledig gehallucineerde antwoorden, met mogelijk ernstige nefaste impact. Bijvoorbeeld, Air Canada [werd in het begin van 2024 verplicht](#) om een gehallucineerde terugbetaling policy na te leven. In dit thema werken we rond drie gevastigde methoden om de precisie van responses te verhogen: (1) Prompt-engineering technieken zoals chain-of-thought, instruction fine-tuning en contrastive reasoning. (2) Het dynamische ophalen van relevante kennis en die gebruiken om de context te verrijken, i.e., Retrieval-Augmented Generation (RAG). (3) Fine-tuning van het model met eigen data. Hier zullen we technieken behandelen zoals traditionele fine-tuning, Low-Rank Adaptation (LoRA), en het leren van een eigen fine-tuning beloningsfunctie m.b.v. Reinforcement Learning from Human Feedback (RLHF) gedreven door in-house experts. Ook praktische implementatiekeuzes worden hier behandeld (bv. LLM-service vs. eigen infrastructuur, cloud vs. local, large language model vs. small language model, GPT4 vs. LLama3 vs. Phi-3 vs. ...).

Het tweede deel richt zich op de veiligheidsaspecten van LLM's. Het gebruik van machine learning in softwareapplicaties vergroot het aanvalsoppervlak. Kwetsbaarheden in machine learning worden al een decennium bestudeerd binnen het domein van Adversarial Machine Learning. In dit domein zijn aanvallen ontwikkeld die alle aspecten van de CIA-triade (Confidentiality, Integrity, Availability) bestrijken en kunnen worden uitgevoerd tijdens de ontwikkelings- en operationele fase van een ML-systeem. Bovendien zorgt de integratie van LLM's in applicaties voor aanzienlijke uitdagingen, omdat het onmogelijk is om in een LLM data van instructies te scheiden. Dit kan leiden tot indirecte prompt-injectie-aanvallen, zoals een vraag over het weer die een [phishinglink genereert binnen de Bing Search Copilot](#), of de [exfiltratie van gegevens in Google Docs via Google Gemini](#). Dit deel zal meer inzicht geven in hoe dergelijke kwetsbaarheden zich manifesteren en vervolgens de meest geavanceerde oplossingen bespreken. Eerst zullen we het concept van LLM's verduidelijken, gevolgd door een bespreking van referentieaanvalspatronen uit het veld van Adversarial Machine Learning. Concrete kwetsbaarheden van op LLM's gebaseerde applicaties zullen worden besproken aan de hand van referentieraamwerken zoals de de [OWASP LLM top 10](#) en [MITRE ATLAS](#). Tot slot zullen we concrete voorstellen doen voor een defense-in-depth aanpak, waarbij specifieke strategieën en tools voor [threat modeling](#), [AI red teaming](#), [zelf moderatie](#) en [AI guardrails](#) aan bod komen.

Het derde deel richt zich op de uitrol en werking van de LLM, het onderhoud, en de impact op de CI/CD pipeline (het geheel wordt ook wel *LLMOps* genoemd). Dit deel bouwt verder op de implementatie-aspecten die in het eerste deel besproken worden en verzekert de soepele, correcte werking van LLM's in productie. In dit thema wordt gewerkt rond de stappen in het LLMOps proces: (1) Er worden usecase-specifieke tools en metrieken geïntroduceerd om de performantie van het model te meten (bv. [ROUGE](#) voor usecase 2, [BLEU](#) voor usecase 3), om eventuele bias te testen (bv. [TruLens](#)), en applicatie-specifieke scenario's te testen. (2) De deployment-processen worden geautomatiseerd d.m.v. een volledige integratie in de CI/CD pipeline. Dit omvat uitrol van zowel lokale modellen en LLM-services naar on-premise of cloud-gebaseerde infrastructuur. (3) LLM's in productie moeten voortdurend gemonitord worden om hun correcte werking te verzekeren. Er moet inhoudelijk gecontroleerd worden dat de antwoorden van de LLM in lijn liggen met de doelen van de usecase, maar ook niet-functievere vereisten, zoals het detecteren van aanvallen, in rekening brengen van de lopende kosten, en verzekeren van de beschikbaarheid van de service (en eventueel opschalen van de service), moeten afgedekt worden. We introduceren hier specifieke tools voor (bv. [Langkit](#))

Het vierde en laatste deel behandelt de complexe juridische aspecten en ethische uitdagingen die gepaard gaan met het gebruik van LLM's. Eerder dit jaar heeft het Europese parlement de AI Act goedgekeurd, de eerste AI-wetgeving in de wereld. We scheppen duidelijkheid over de impact van deze wetgeving op bedrijven, zowel op juridisch vlak (*wat moet ik doen*) als technisch vlak (*hoe moet ik dat doen*). Ook relevante bestaande wetgeving wordt op dezelfde manier behandeld. De privacy- en gegevensbeschermingsregels uit de AVG worden besproken in de context van het trainen van LLM's. De Digital Services Act (DSA) wordt besproken omdat die bedrijven verplicht duidelijkheid te verschaffen over het gebruik van AI en verantwoordelijkheid te dragen voor door AI beïnvloede beslissingen. En tot slot moeten bedrijven, overeenkomstig Europese regelgeving, intellectuele eigendom beschermen, waarbij specifieke maatregelen dienen te worden genomen om auteursrechten te waarborgen.

Om al deze informatie naar de doelgroep te brengen, doen we aan kennisoverdracht op verschillende manieren (seminaries, demonstraties, workshops, brede outreach) en zorgen we voor persistente resultaten (beslissingsraamwerken, referentie-architecturen, assessments, voorbeeldcode, threat models, best practices, ...) die publiek beschikbaar gemaakt worden op de projectsite. Het werkplan van het project is ingedeeld in werkpakketten volgens de verschillende projectaspecten (onderzoek, vertaalonderzoek, kennisoverdracht, ...). Bijgevolg komt elk van de vier projectdelen terug in elk van de onderstaande werkpakketten. Een gedetailleerd overzicht van de werkpakketten volgt hieronder, met op het einde van deze sectie een overzicht van alle leverbaarheden.

<i>WP nummer:</i>	0	<i>beginmaand:</i>	1	<i>duurtijd (maand)</i>	24	<i>totaal aantal mensmaanden</i>	4.2							
<i>Titel:</i>	Projectmanagement													
<i>Werkpaketleider:</i>	<b>Sirris</b>													
<i>Betrokken partner:</i>	<i>DistriNet</i>	<i>Sirris</i>												
<i>Mensmaanden:</i>	2	2.2												
<b>Onderaannemer(s):</b>	/													
<b>Doelstellingen:</b>	Opvolging en sturing van het project voor het tijdig opleveren van deliverables, rapportering, communicatie met de begeleidingsgroep en implementaties in deel B te verzekeren.													
<b>Taken: beschrijving van de activiteiten, ...</b>														
Taak 1:	<b>Projectmanagement</b> Coördinatie van de vooruitgang in de werkpakketten en het stimuleren van de samenwerking tussen de werkpakketten en de projectpartners, en de organisatie van stuurgroepen op regelmatige basis.													
Taak 2:	<b>Coördinatie en opvolging van de begeleidingsgroep</b> Overleggen met de begeleidingsgroep zodat de collectieve ontwikkelingen en kennistransfer optimaal inspelen op de industriële noden van de brede doelgroep, en stimuleren van concrete implementatie van de opgedane kennis.													
Taak 3:	<b>Projectrapportering</b> Administratieve opvolging en rapportering van projectresultaten aan VLAIO en projectpartners													
<b>Verwachte resultaten en leverbaarheden</b>														
Statusrapporten: rapportering voor de verschillende WP's, monitoring van de planning, voortgang en risico's in het project, status van de begeleidingsgroep en de ondernemingsspecifieke cases, wijzigingen in het project, etc. (elke 6 maanden)														

<b>WP nummer:</b>	1	<b>beginmaand:</b>	1	<b>duurtijd (maand)</b>	15	<b>totaal aantal mensmaanden</b>	11.4
<b>Titel:</b>	Kennisopbouw en -vergaring						
<b>Werkpakketleider:</b>	<b>DistriNet</b>						
<b>Betrokken partner:</b>	<i>DistriNet</i>	<i>Sirris</i>					
<b>Mensmaanden:</b>	7	4.4					
<b>Onderaannemer(s):</b> /							
<b>Doeleinden:</b>	<p>Dit werkpakket richt zich op het verankeren van kennis over het gebruik van LLM's, waaronder technische aanpakken en tools voor zowel functionele als security testing, en het integreren van die tools in de ontwikkelingscyclus. Een aantal aspecten die mee in overweging zullen genomen worden, zijn:</p> <ul style="list-style-type: none"> <li>○ <i>De toepasbaarheid van de tools en technologieën m.b.t. LLM-integraties</i></li> <li>○ <i>De mogelijkheid tot integratie in de SDLC (met een focus op automatisatie)</i></li> <li>○ <i>De leercurve van de tools of technieken</i></li> </ul>						
<b>Taken: beschrijving van de activiteiten, ...</b>							
Taak 1:	<p><b>Exploratie van technologieën i.v.m. LLM-implementatietechnieken</b> Deze kennis zal geconcretiseerd worden door mogelijke varianten van alternatieve technieken te documenteren en blauwdrukken op te stellen die bedrijven zullen toelaten de juiste keuzes voor technologie en tools te maken.</p>						
Taak 2:	<p><b>Exploratie van technologieën i.v.m. functionele en security testing van LLM's</b> Er worden concrete evaluation grids en trade-off analyses gemaakt die bedrijven zullen helpen om de juiste functionele en security testing tools te kiezen.</p>						
Taak 3:	<p><b>Exploratie van AI governance en regelgeving</b> Documenteren van de typische governance vereisten voor AI-systemen, met een specifieke nadruk op potentiële juridische valkuilen.</p>						
<b>Verwachte resultaten en leverbaarheden</b>	3 white papers met blauwdrukken om de juiste keuze te maken m.b.t. implementatietechnieken, functionele testing en security testing, en de governance-eisen die stakeholders stellen (M12)						

<b>WP nummer:</b>	2	<b>beginmaand:</b>	4	<b>duurtijd (maand)</b>	12	<b>totaal aantal mensmaanden</b>	13.3							
<b>Titel:</b>	Vertaling van kennis naar industrie-gedreven usecases													
<b>Werkpakketleider:</b>	<b>DistriNet</b>													
<b>Betrokken partner:</b>	DistriNet	Sirris												
<b>Mensmaanden:</b>	8.9	4.4												
<b>Onderaannemer(s):</b>	/													
<b>Doelstellingen:</b>	<p>In overleg met de begeleidingsgroep worden implementatievarianten gedefinieerd en trade-offs geanalyseerd om tegemoet te komen aan de behoeften van bedrijven. Op basis van deze varianten worden dan trade-off analyses gemaakt en concrete sjablonen uitgewerkt.</p>													
<b>Taken: beschrijving van de activiteiten, ...</b>														
Taak 1:	<p><b>Definitie van implementatievarianten</b> In overleg met de begeleidingsgroep worden architecturale implementatievarianten gedefinieerd die representatief zijn voor de applicaties die de bedrijven ontwikkelen (bv. andere gebruikersinterfaces, output filtering, interactie met gebruikers, ...). De voornaamste eisen worden in kaart gebracht, waarna 2 specifieke architecturale varianten gedefinieerd worden die de noden van meerdere partners in de begeleidingsgroep afdekken.</p>													
Taak 2:	<p><b>Trade-off analyses</b> Vertrekend van de kennis uit WP1 zal voor elk van de varianten (cfr. Taak 1) de trade-offs in kaart gebracht worden (bv. grote of kleine taalmodellen, cloud of local, veiligheid, performantie, kosten, ...). Deze trade-offs worden geanalyseerd volgens een evaluatieframework om op die manier complexe keuzemogelijkheden te vereenvoudigen.</p>													
Taak 3:	<p><b>Opstellen van sjablonen die helpen m.b.t. governance</b> De resultaten uit WP1 (Taak 3) worden gecombineerd met de reële implementaties van de bedrijven in de begeleidingsgroep, waaruit 2 specifieke sjablonen opgesteld worden, elk met een andere focus, namelijk de technieken die gebruikt worden om de veiligheid van de integratie te garanderen enerzijds, en de toolingstrategie die instaat voor het garanderen van de veiligheid en correctheid tijdens het deploymentproces anderzijds.</p>													
<b>Verwachte resultaten en leverbaarheden</b>														
<ul style="list-style-type: none"> <li>○ <i>Beschrijving van 2 architecturale varianten van LLM-integraties (M9)</i></li> <li>○ <i>Proof-of-concept demonstrators (een voor elke architecturale variant) (M11)</i></li> <li>○ <i>Trade-off analyse per architecturale variant (M15)</i></li> <li>○ <i>2 sjablonen m.b.t. de rapportage van de gekozen integratie-architectuur en tijdens het deploymentproces in een governance context (cybersecurity/privacy) (M15)</i></li> </ul>														

<b>WP nummer:</b>	3	<b>beginmaand:</b>	7	<b>duurtijd (maand)</b>	18	<b>totaal aantal mensmaanden</b>	13.5
<b>Titel:</b>	Kennisoverdracht						
<b>Werkpakketleider:</b>	<b>Sirris</b>						
<b>Betrokken partner:</b>	<i>DistriNet</i>	<i>Sirris</i>					
<b>Mensmaanden:</b>	7.9	5.6					
<b>Onderaannemer(s):</b>	/						
<b>Doelstellingen:</b>	<p>De projectpartners organiseren interactieve seminars en workshops waarin bedrijven, de academische wereld en de begeleidingsgroep samenkommen om state-of-the-art technologieën, best practices en ervaringen met het integreren van LLM-technologie te delen. Demonstraties van relevante tools worden gegeven en groepscoachingssessies helpen bij het analyseren van keuzemogelijkheden en trade-offs, waardoor weloverwogen en veilige beslissingen genomen kunnen worden.</p>						
<b>Taken: beschrijving van de activiteiten, ...</b>							
Taak 1:	<p><b>Interactieve seminars</b> De projectpartners organiseren interactieve seminars waarin bedrijven en de academische wereld samenkomen om specifieke onderwerpen te bespreken. Deze seminars omvatten ook thematische ervaringsdeskundigen en <i>experience reports</i> van leden van de begeleidingsgroep, gebaseerd op hun ervaringen met ondernemingsspecifieke cases. De deelnemers zullen waardevolle inzichten opdoen in state-of-the-art LLM-technologieën, de nieuwste ontwikkelingen en best practices, en relevante wetgeving.</p>						
Taak 2:	<p><b>Demonstraties van specifieke technologieën</b> De projectpartners geven demonstraties van tools en technologieën die relevant zijn voor de concrete softwareimplementaties van de bedrijven. Dit kan bijvoorbeeld een generieke aanpak zijn om de implementatie en het veilige gebruik van LLM's te integreren in het ontwikkelingsproces, of kan een specifieke tool zijn voor een technologie die door verschillende leden van de begeleidingsgroep gebruikt wordt.</p>						
Taak 3:	<p><b>Hands-on workshops met specifieke technologieën</b> De projectpartners organiseren interactieve workshops waar deelnemers hands-on praktijkervaring en kennis kunnen opdoen over state-of-the-art methoden en specifieke technologieën voor het veilig implementeren van LLM's.</p>						
Taak 4:	<p><b>Groep-coaching rond analyse van trade-offs</b> De projectpartners zullen groepscoachingssessies organiseren waarin de representatieve usecases worden geanalyseerd en waarin er dieper wordt ingegaan op het onderzoeken van keuzemogelijkheden en trade-offs. Deze coachingssessies zullen gebruikmaken van het evaluatieraamwerk en de instantiatie ervan aan de hand van de usecases, zodat de begeleidingsgroep in staat zal zijn om weloverwogen en veilige keuzes te maken, rekening houdend met de voor- en nadelen.</p>						

### **Verwachte resultaten en leverbaarheden**

Adviezen en analyserapporten, interactieve seminars (min. 5), demonstraties (min. 1), workshops (min. 1), coaching sessies, ... afhankelijk van de noden van de begeleidingsgroep. (start in M7)

<i>WP nummer:</i>	4	<i>beginmaand:</i>	13	<i>duurtijd (maand)</i>	12	<i>totaal aantal mensmaanden</i>	6.9
<i>Titel:</i>	Brede disseminatie en outreach						
<i>Werkpakketleider:</i>	<b>DistriNet</b>						
<i>Betrokken partner:</i>	<i>DistriNet</i>	<i>Sirris</i>					
<i>Mensmaanden:</i>	2.5	4.4					
<b>Onderaannemer(s):</b>	/						
<b>Doelstellingen:</b>	<p>Het doel van dit werkpakket is om kennis en projectresultaten naar een breder publiek te verspreiden, zoals bijvoorbeeld onderzoekers, beveiligingsspecialisten, full-stack applicatieontwikkelaars en andere belanghebbenden. Dit zal worden bereikt via diverse kanalen, zoals portals, websites, deelname aan industriële evenementen, publicatie van whitepapers en wetenschappelijke/populariserende artikelen, demonstratie van proof-of-concept oplossingen via portals, en het organiseren van workshops en presentaties.</p>						
<b>Taken: beschrijving van de activiteiten, ...</b>							
Taak 1:	<p><b>Publiek-beschikbare naslagwerken, whitepapers, <i>evaluation grids</i> en implementatievoorbeelden</b></p> <p>Deze taak zal leiden tot het creëren van rapporten of whitepapers die publiekelijk toegankelijk zijn, evenals voorbeelden van het toepassen van de evaluation grids op representatieve usecases. Hierdoor wordt het mogelijk om de opgedane kennis en expertise over het koppelen van verschillende technologieën aan een breder publiek beschikbaar te maken.</p>						
Taak 2:	<p><b>Publieke outreach via seminars, workshops, conferenties en andere events</b></p> <p>De focus van deze taak ligt op het uitdragen van de expertise van het consortium door deelname aan wetenschappelijke workshops en conferenties, industriële evenementen, en het organiseren van presentaties tijdens specifieke evenementen gericht op cyberveiligheid in de softwareontwikkelingscyclus.</p>						
<b>Verwachte resultaten en leverbaarheden</b>	<ul style="list-style-type: none"> <li>○ <i>Publiek beschikbare whitepapers met evaluation grids en implementatievoorbeelden (doel: 10) (M13)</i></li> </ul> <p>Publieke outreachactiviteiten (doel: 4) (M13)</p>						

<i>WP nummer:</i>	5	<i>beginmaand:</i>	13	<i>duurtijd (maand)</i>	12	<i>totaal aantal mensmaanden</i>	2.1
<b><i>Titel:</i></b>	Valorisatie faciliteren						
<b><i>Werkpakketleider:</i></b>	<b>Sirris</b>						
<b><i>Betrokken partner:</i></b>	<i>DistriNet</i>	<i>Sirris</i>					
<b><i>Mensmaanden:</i></b>	1	1.1					
<b>Onderaannemer(s):</b>	/						
<b>Doelstellingen:</b>	<p>Het doel van dit werkpakket is het plannen en ondersteunen van de kennisvalorisatie binnen het kader van dit project. Het omvat twee taken: het creëren van een langetermijnprojectsuite voor het delen van kennis en ervaringen met een breed publiek, en het monitoren van ontwikkelingen in het technologielandschap om uitdagingen op het gebied van de veilige en performante integratie van LLM's aan te pakken.</p>						
<b>Taken: beschrijving van de activiteiten, ...</b>	<p><b>Taak 1:</b> <b>Voorbereiding tot lange-termijn kennisbank rond veilige en performante integratie van LLM-technologie</b>        Deze taak is gericht op het voorbereiden van de langdurige beschikbaarheid van kennis en expertise in een projectsuite die al tijdens de looptijd van het project als kennisbank fungeert en ook na afloop van het project beschikbaar blijft. Er worden experience reports en praktijkverhalen verzameld om een bredere groep bedrijven te kunnen bereiken. Daarnaast wordt de projectsuite aangevuld met voorbeeldimplementaties en proof-of-concept-oplossingen, zodat ze nuttig kan zijn bij het opstarten van specifieke bedrijfscases op lange termijn.</p> <p><b>Taak 2:</b> <b>Innovation watch &amp; opportunity identification</b>        Deze taak houdt de ontwikkelingen bij op het gebied van de uitdagingen, problemen en oplossingen in een snel veranderend technologielandschap. Door continu veranderingen in het LLM-ecosysteem in kaart te brengen, zal deze taak eventuele projectaanpassingen en mogelijke vervolgactiviteiten identificeren, die kunnen leiden tot de opstart van nieuwe projecten buiten de context van dit COOCK+-project.</p>						
<b>Verwachte resultaten en leverbaarheden</b>	Projectsite (M13)						

### Overzichtstabel van de mensmaanden per partner en per werkpakket

<b>WP</b>	<b>Partner</b>	<b>Jaar 1</b>	<b>Jaar 2</b>	<b>TOTAAL</b>
<b>0</b>	Sirris	1.1	1.1	2.2
	DistriNet	1	1	2
<b>1</b>	Sirris	3.5	0.9	4.4
	DistriNet	6	1	7
<b>2</b>	Sirris	3.3	1.1	4.4
	DistriNet	6.9	2	8.9
<b>3</b>	Sirris	2.8	2.8	5.6
	DistriNet	2.1	5.8	7.9
<b>4</b>	Sirris	0	4.4	4.4
	DistriNet	0	2.5	2.5
<b>5</b>	Sirris	0	1.1	1.1
	DistriNet	0	1	1
<b>TOTAAL</b>		<b>26.7</b>	<b>24.7</b>	<b>51.4</b>

### Overzicht van de belangrijkste leverbaarheden en de voorziene timing

<b>Omschrijving leverbaarheden</b>	<b>Hoofdcategorie</b>	<b>Voorziene timing (maand)</b>
<b>Projectspecifieke kennisontwikkeling</b>		
3 whitepapers met blauwdrukken om de juiste keuze te maken m.b.t. implementatietechnieken, functionele testing en security testing, en de governance-eisen die stakeholders stellen	X1	12
2 architecturale varianten van LLM-integraties	X1	9
Proof-of-concept demonstrators (per architecturale variant)	X3	11
Trade-off analyses (per architecturale variant)	X2	15
2 sjablonen m.b.t. de rapportage van de gekozen integratie-architectuur en tijdens het deploymentproces in een governance context (cybersecurity/privacy en andere regelgeving)	X1	15
<b>Collectieve/generieke kennisoverdracht</b>		
Adviezen, analyserapporten en coachingssessies	Y3	13

Interactieve seminaries (min. 5), demonstraties (min. 1), interactieve workshops (min. 1)	Y5	7
Publiek beschikbare white papers met evaluation grids en implementatievoorbeelden (doel: 10)	Y3	13
Publieke outreachactiviteiten (doel: 4)	Y5	13
Projectsite	Y4	13

#### 4. Middelen en Expertise

De samenwerking tussen DistriNet en Sirris omvat de volledige waardeketen, van fundamenteel onderzoek tot industriële implementatie. DistriNet kan met hun onderzoeksexpertise bijdragen aan de ontwikkeling van geavanceerde technieken op het gebied LLM's, waarbij in eerste plaats hun focus ligt op het beveiligen van LLM's, maar ook bij het uitrollen en integreren van deze technologieën in software. Sirris kan vervolgens hun industriële expertise toepassen om deze resultaten mee over te dragen naar bedrijven en kan hen ondersteunen bij het bouwen en implementeren van beveiligde LLM-gebaseerde softwareoplossingen. Hierdoor wordt de impact van de samenwerking vergroot.

De kernpersonen in dit dossier zijn:

- **Nick Boucart** werkt als senior technologie-adviseur bij Sirris, waar hij software-ondernemers helpt met het opzetten van data-gedreven product management, (cloud) architecturen, en advies rond software engineering in het algemeen. Recent lag Nick mee aan de basis voor de masterclass cybersecurity voor bouwers van digitale diensten. Nick is mede-auteur van het boek "Hyperscale and Microcare - the digital business cookbook"
- **Niels Holvoet** is een gepassioneerde technoloog bij Sirris met expertise in digitaal productbeheer, DevSecOps-praktijken en generatieve AI-oplossingen. Niels staat aan de frontlinie van het verkennen van het transformatieve potentieel van generatieve AI en ontwikkelt actief co-pilot prototypes voor klanten. Hij heeft een succesvolle staat van dienst in het begeleiden van Belgische bedrijven door innovatieprocessen, waarbij hij strategisch advies en coaching biedt voor de ontwikkeling van digitale producten en diensten. Als voorvechter van de integratie van beveiliging heeft Niels ervaring met het integreren van geavanceerde beveiligingstools in CI/CD-pijplijnen, waardoor vroege detectie en preventie van kwetsbaarheden wordt verzekerd.
- **Wim Codenie** werkt als senior advisor digital business bij Sirris. Hij heeft ervaring met software bedrijven en heeft meegewerk aan verschillende projecten van Sirris in het domain van digitale innovatie. Recent heeft hij meegewerk aan de basis van het uitwerken van de GenAI visie van Sirris.
- **Dr. Sreeraj Rajendran** is een Senior Data Scientist bij Sirris, waar hij leiding geeft aan de Distributed Intelligence Cluster van het Data and AI Competency Lab. Hij superviseert innovatieve projecten op het gebied van gedistribueerde AI, generatieve AI en geavanceerde voorspellingen in de verkeers- en energiesector. Met een PhD in Ingenieurswetenschappen van KU Leuven heeft hij een sterke achtergrond in deep learning-oplossingen voor grootschalige draadloze spectrum monitoring. Zijn carrière omvat een postdoctoraal onderzoekspositie aan KU Leuven, gericht op machine learning voor draadloze communicatie en laagvermogen sensornetwerken, en een rol als Senior Design Engineer bij Cadence Design,

*waar hij DSP-algoritmen implementeerde op vectorprocessoren. Hij heeft ook een masterdiploma in Elektrotechniek van IIT Bombay, India, met specialisatie in draadloze communicatie en signaalverwerking.*

- *Laurens Le Jeune, PhD, werkt als security en data scientist bij Sirris. Hij heeft expertise in de detectie van indringers in computernetwerken met behulp van artificiële intelligentie en hardwareversnelling. Binnen Sirris werkt hij vooral in (inter)nationale R&D projecten met industrie in de intersectie tussen cybersecurity en artificiële intelligentie.*
- *Prof. dr. ir. Lieven Desmet is hoofddocent binnen de onderzoeksgroep DistriNet, en bestudeert er beveiligings- en privacy-aspecten in software en systemen. In de afgelopen 10 jaar heeft Lieven een onderzoeksteam uitgebouwd binnen DistriNet op het raakvlak tussen security/privacy en machine learning. Enerzijds realiseert dit team, steunend op machine learning technieken, verbeterde security en privacy oplossingen in een waaier van security domeinen gaande van network intrusion detection en malware tot DNS abuse en phishing. Anderzijds focust dit team zich op het beschermen van ML-gebaseerde oplossingen tegen security en privacy aanvallen, en het meer robust maken van ML-gebaseerde oplossingen in realistische operationele contexten. Meer recent bestudeert dit onderzoeksteam ook de security en privacy aspecten bestudeert bij integratie van LLMs in bedrijfstoepassingen.*
- *Dr. Vera Rimmer is een onderzoeksexpert bij DistriNet. Ze bestudeert cybersecurity en privacy-versterkende technologieën; toegepaste machine learning en deep learning; privacy en betrouwbaarheid van toegepaste data-gedreven AI. Haar onderzoek verkent deep learning als een bedreiging tegen anonieme communicatie, en verschillende aspecten van door AI mogelijk gemaakte inringingsdetectie en authenticatie. Vera is in het bijzonder geïnteresseerd in het ontwikkelen van een alomvattend begrip, redelijke verwachtingen en het beperken van risico's van data-gedreven AI.*
- *Dr. Pieter Philippaerts werkt als onderzoeksmanager bij de DistriNet onderzoeksgroep. Hij richt zich voornamelijk op onderzoek binnen het brede domein van applicatiebeveiliging, met een bijzondere focus op het ontwerpen van praktische securitytooling.*

Naast de industriële toepassings- en onderzoeksexpertise binnen Sirris en DistriNet, kan ook gerekend worden op externe partners met gespecialiseerde kennis om eventuele hiaten bij de projectpartners te dichten. Zo zal er bijvoorbeeld beperkt beroep gedaan worden op de deskundigheid van het Centre for IP & Law (CiTiP, KU Leuven) om zeer technisch-juridische analyses te maken van de komende AI-wetgeving.

#### MIDDELEN

De gevraagde middelen zullen overwegend aangewend worden voor personeel. De huidige begroting in mensmaanden is minimaal maar voldoende voor de beoogde taken en dit met een gezonde mix van junior en senior mensen.

We zijn ervan overtuigd de nodige cofinanciering te zullen halen via de cases, maar ingeval we een lagere financieringsgraad zouden bekomen, zal elke partner pro rata eigen middelen aanwenden.

## 5. Economische impact

Het project heeft voor softwareontwikkelaars (en indirect voor hun klanten) een grote economische impact. We analyseren de impact vanuit drie perspectieven.

### Algemene economische groei

Uit [een analyse van de Europese Rekenkamer](#) blijkt dat investeringen in AI-technologie grote economische voordelen zullen opleveren voor Europese regio's, waaronder Vlaanderen. AI draagt bij aan verbeterde efficiëntie, innovatie en concurrentievermogen van bedrijven. Door te investeren in projecten zoals het LISA-project, krijgen Vlaamse bedrijven een voordeel om die geavanceerde technologieën sneller in de bedrijfsprocessen te integreren en zo nieuwe markten te ontsluiten.

De Rekenkamer wijst erop dat AI niet alleen de kosten verlaagt en de operationele efficiëntie verbetert, maar ook nieuwe banen creëert en economische groei stimuleert. Dit is essentieel voor Vlaanderen, waar de economie sterk afhankelijk is van technologische innovatie. Bovendien kan AI helpen om de verdere digitalisering van de economie te versnellen, wat cruciaal is voor het behoud van de internationale concurrentiepositie van Vlaanderen. Een project zoals LISA ligt dus volledig in lijn met [de Europese ambitie](#) omtrent het opzetten van een sterk AI-ecosysteem.

### **Vermindering van de kosten**

Het LISA-project zal naar verwachting leiden tot een versnelde go-to-market van bedrijven in onze doelgroep, dankzij de kennisopbouw en -vertaling. Enerzijds zullen de resultaten van het project helpen bij het oplossen van technische moeilijkheden waarmee bedrijven in de doelgroep te maken hebben bij het implementeren en integreren van LLM-toepassingen op een veilige manier. Anderzijds zullen de specifieke demonstratoren en trade-off analyses bijdragen aan een snellere implementatie van een volwaardig en veilig product.

Voor ondernemingen die hun specifieke case tot stadium 4 of 5 brengen, verwachten we dankzij de projectresultaten een snelheidswinst van 2–6 kwartalen (afhankelijk van welke onderdelen ze uit het project overnemen). De trade-off analyses en de demonstratoren zullen bijdragen tot het efficiënter bepalen van de juiste technologiekeuzes die gepast zijn voor de onderneming. Anderzijds zullen de architecturale blauwdrukken een aanzienlijke versnelling genereren bij het analyseren en verbeteren van de ondernemingsspecifieke implementatie.

### **LLM's als sales enabler**

De kennisopbouw binnen het LISA-project zal de softwareontwikkelaars in staat stellen de verkoopcycli te verkorten en de commerciële slaagkans te verhogen. Zeker in een B2B context, waar de verkoopcyclus gemiddeld 2 tot 4 kwartalen bedraagt, verwachten we dat onze doelgroep hun verkoopcyclus zou kunnen verkorten. We verwachten ook dat bedrijven die proactief genAI (en LLM's in het bijzonder) inzetten in hun producten een verhoging van de conversiegraad van hun verkoop kunnen realiseren, wat leidt tot groei en meer tewerkstelling. De totale valorisatie van een hogere graad van vertrouwen is uiteraard moeilijk te kwantificeren, en gaat immers ook veel verder dan enkel maar de impact op verkoop.

Een groot deel van de bedrijven in de begeleidingsgroep zijn groeidistricten: ze gebruiken innovatie en het vergroten van hun toegevoegde waarde (het naar de markt brengen van nieuwe en/of verbeterde producten) als een van de drijvende krachten om die groei te realiseren. Voor bedrijven die sterk willen inzetten op AI en het als verkoopargument willen uitspelen verwachten we dat ze sneller als "sterk merk" aanzien zullen worden. Een snellere ontwikkeling van veilige software zorgt eveneens voor een competitief voordeel in de internationale markt.

We verwachten geen interne/externe obstakels (zoals intellectueel eigendom of wetgeving) die de economische impact kunnen hinderen of vertragen. Het aanbod van technologieën op de markt kan echter snel veranderen, maar onze projectaanpak houdt rekening met deze realiteit. Door voortdurend nieuwe technologieën en benaderingen te screenen met behulp van onze experts en deze analyse op te nemen in

de kennisoverdracht, zorgen we ervoor dat bedrijven in de begeleidingsgroep vroegtijdig toegang hebben tot kwalitatieve technologieën. Dit verzekert hen van een voorsprong op dit gebied.

## 6. Kennisverspreiding

Het project beoogt kennisverspreiding en impact op meerdere delen van de waardeketen, van ontwikkeling tot implementatie en onderhoud van LLM-gebaseerde oplossingen. Door de integratie van best practices uit software engineering en DevOps toe te passen in de context van Large Language Models (LLM's), worden de competenties van softwareontwikkelaars versterkt. De kennis blijft niet alleen theoretisch door die ook toe te passen op realistische scenario's (aangebracht door de bedrijven in de begeleidingsgroep, waar mogelijk). Het project faciliteert de overgang van proof-of-concept naar productieklare systemen, met aandacht voor prestatie, kostenbeheer, betrouwbaarheid en veiligheid.

Tijdens het project focust de disseminatiestrategie op een combinatie van seminars, workshops, whitepapers, en interactieve demo's. Daarnaast ontwikkelen we een online kennisportaal waar alle projectuitkomsten en aanbevelingen toegankelijk zijn voor een breder publiek. Na afloop van het project wordt het kennisportaal omgezet in een langetermijnkenniscentrum, dat fungeert als een centraal verdeelpunt voor de opgebouwde kennis en de ontwikkelde deliverables. Dit centrum wordt een bron van up-to-date informatie en best practices voor Vlaamse bedrijven, zodat zij blijvend kunnen profiteren van de inzichten en technieken die ontwikkeld werden tijdens het project.

## 7. Ruimere meerwaarde

### **Maatschappelijke meerwaarde**

Volgens ons heeft dit project mogelijk een zeer grote hefboom en positief maatschappelijk effect. Artificiële intelligentie zal in de toekomst overal geïntegreerd worden. Door bedrijven bewust te laten worden van de potentiële problemen, zowel op beveiligings- als privacygebied, zorgen we ervoor dat de afgeleverde producten al van bij het begin voldoen aan de gewenste en de vereiste standaarden. Het project helpt om LLM's te transformeren tot "sales enabler" voor de deelnemende bedrijven, waardoor die technologieën doorstromen naar de gebruikers van die software en de maatschappij in zijn geheel. We zijn ervan overtuigd dat het omarmen van artificiële intelligentie een trein is die vertrokken is, en niet meer te stoppen. De meeste bedrijven hebben deze trend nog niet opgemerkt of weten niet hoe hiermee op positieve wijze om te gaan. Met de ervaringen en de uitgewerkte cases in dit project willen we hen duiding geven.

### **Risico op marktverstoring**

Aangezien de kennis die in dit project opgebouwd wordt nog niet (gecentraliseerd) beschikbaar is, zal dit project eerder marktcreërend werken dan marktverstorend. Door het opzetten van een lang termijn kenniscentrum waarop alle informatie vrij beschikbaar en herbruikbaar is, verzekeren we de doorstroming van de opgebouwde kennis naar de markt toe. Dit verhoogt de schaalbaarheid en het bereik van de projectresultaten aanzienlijk, ook na het officiële einde van het project. Dienstverleners zijn vrij om het materiaal te gebruiken om (op dit moment nog onbestaande) opleidingen te ontwikkelen die dan verder kunnen aangeboden worden aan bedrijven die nood hebben aan extra hulp.

**VLAIO**

Koning Albert II-laan 35 bus 12  
1030 Brussel  
[www.vlaio.be](http://www.vlaio.be)