provincie limburg

Data Protection Impact Assessment (DPIA)

Limburgse AI Chat Assistent (LAICA)

GovChat-NL V3

provincie limburg

Vaststelling

Verwerkingsverantwoordelijke: 12 maart 2025

Naam: [redacted]

Advies functionaris voor gegevensbescherming: 13 maart 2025

Naam: [redacted]

Versie: 1.1

Status: Definitief

Revisie:

Versie	Datum	Toelichting
Versie 0.1	15 november 2024	Concept omschrijving voorstel, persoonsgegevens en gegevensverwerkingen en eerste aanzet verwerkingsdoeleinden en betrokken partijen.
Versie 0.2	27 november	Verwerking feedback overleg 25 november met [redacted]
Versie 0.3	14 januari 2025	Verwerking opmerkingen FG
Versie 1.0	22 januari 2025	Definitief V2
Versie 1.1	12 maart 2025	Aanpassingen voor V3

provincie limburg

Inhoudsopgave

Inleiding

LAICA is een AI-chatassistent ontwikkeld door het cluster Organisatie & Informatie (O&I) van de Provincie Limburg. Het staat voor Limburgse AI Chat Assistent. LAICA is ontworpen als een hulpmiddel om ambtenaren te ondersteunen bij hun dagelijkse werkzaamheden. Deze DPIA onderzoekt de gevolgen voor de bescherming van persoonsgegevens bij het gebruik van de LAICA.

LAICA maakt gebruik van een aantal standaardvoorzieningen die de Provincie ter beschikking heeft, zoals Entra ID voorheen AAD (Azure Active Directory) en internetbrowsers. Hierin zijn ook privacy gerelateerde zaken opgenomen die in deze DPIA worden meegenomen, omdat er nog geen afzonderlijke DPIA bestaat voor deze componenten binnen de Provincie Limburg.

LAICA maakt gebruik van AAD voor authenticatie en autorisatie. AAD is een cloud-gebaseerde identiteits- en toegangsbeheerdienst die wordt aangeboden door Microsoft. Door het gebruik van AAD voor authenticatie en autorisatie wordt de beveiliging van LAICA versterkt en wordt ervoor gezorgd dat alleen geautoriseerde gebruikers toegang hebben tot het systeem. Het biedt ook mogelijkheden voor het beheer van gebruikersidentiteiten en toegangsrechten op een centrale en gestructureerde manier. Implementatie en configuratie van AAD in LAICA is afhankelijk van de keuzes en richtlijnen van het cluster O&I van de Provincie Limburg. Deze kunnen variëren afhankelijk van de vereisten en beveiligingsstandaarden van de organisatie. Aspecten m.b.t. AAD zijn wel opgenomen in deze DPIA, omdat er (nog) geen DPIA voor de AAD is.

LAICA is ontworpen als een webgebaseerde AI-chatassistent die toegankelijk is via een webbrowser naar keuze. Hierdoor kunnen gebruikers LAICA benaderen vanaf elke computer of mobiel apparaat met internettoegang, ongeacht het besturingssysteem dat ze gebruiken.

LAICA maakt gebruik van een kennisbank die wordt bijgewerkt door de makers van het informatieproduct. Deze kennisbank bevat informatie over verschillende onderwerpen, zoals wet- en regelgeving, procedures, beleid en andere relevante informatie voor de provincie. De antwoorden die LAICA geeft, zijn gebaseerd op de informatie die beschikbaar is op het moment van de vraag. Als er nieuwe informatie beschikbaar komt, wordt de kennisbank bijgewerkt en kan het antwoord van LAICA veranderen.

Het streven is om LAICA leveranciersonafhankelijk en modulair te maken, wat betekent dat de ontwikkelaars van LAICA zelf verantwoordelijk zijn voor het onderhoud en de verdere ontwikkeling van het systeem, zonder afhankelijk te zijn van externe leveranciers. Dit biedt flexibiliteit en maakt het mogelijk om LAICA beter af te stemmen op de specifieke behoeften van de Provincie Limburg.

LAICA is momenteel gebaseerd op taalmodellen aangeboden vanuit het Microsoft Azure-platform en VertexAI (Google). In de toekomst is het de bedoeling om LAICA ook beschikbaar te maken op andere platforms, zoals Europese / Nederlandse leveranciers, als die er zijn. Dit zou de mogelijkheid bieden om LAICA te gebruiken op verschillende systemen en apparaten, afhankelijk van de voorkeuren en vereisten van de gebruikers. Deze uitbreiding naar andere platforms kan de toegankelijkheid en bruikbaarheid van LAICA vergroten, vendor lock-in voorkomen en het mogelijk maken om snel te kunnen wisselen als de prijs/kwaliteit ergens anders beter is

LAICA is momenteel nog in de testfase en is daarom nog niet beschikbaar voor alle medewerkers. Het doel van de testfase is om LAICA te optimaliseren en de functionaliteit verder uit te breiden op basis van de feedback van gebruikers.

LAICA is een implementatie van het open source project GovChat-NL.

Begrippenlijst:

AI-systemen
AI-systemen of kunstmatige intelligentiesystemen, zijn geavanceerde computerprogramma's die aspecten van menselijke intelligentie nabootsen, zoals leren, probleemoplossing en patroonherkenning. Deze systemen zijn ontworpen om taken uit te voeren die normaal menselijke intelligentie vereisen en worden steeds vaker gebruikt in verschillende toepassingen, van geautomatiseerde klantenservice tot complexe data-analyse.

Taalmodellen, of Large Language Models (LLMs)
Taalmodellen zoals (Chat)GPT zijn geavanceerde AI-systemen die menselijke taal kunnen begrijpen en genereren. Ze worden getraind op grote hoeveelheden tekst, waardoor ze in staat zijn om vragen te beantwoorden, samenvattingen te maken, en zelfs creatief te schrijven. Deze AI-gedreven modellen kunnen worden ingezet om de communicatie, informatievoorziening en interne processen binnen de Provincie Limburg te verbeteren.

Masterprompt
Een masterprompt is een zorgvuldig geformuleerde instructie die aan het begin van een gesprek aan het taalmodel wordt gegeven. Deze sturende instructie bepaalt hoe de chatbot zich gedraagt en beïnvloedt hoe goed het model in staat is om de gebruiker te helpen. Het ontwikkelen van een effectieve masterprompt is een kunst op zich en vereist een diepgaand begrip van zowel de technologie als de behoeften van de gebruiker.

Geparameteriseerde kennis
Geparameteriseerde kennis verwijst naar de informatie die direct in het taalmodel is ingebouwd door de training met grote hoeveelheden tekst. Het model gebruikt deze ingebouwde kennis om vragen te beantwoorden zonder externe bronnen te raadplegen.

Kennisbank
Een kennisbank is een externe database met gestructureerde informatie die het model kan raadplegen. Door gebruik te maken van technieken zoals Retrieval Augmented Generation (RAG), kan het taalmodel relevante informatie uit de kennisbank ophalen voordat het een antwoord genereert, wat leidt tot meer accurate en betrouwbare antwoorden. Het opzetten en onderhouden van een kennisbank is een cruciaal onderdeel van het project, omdat het de kwaliteit en relevantie van de antwoorden van LAICA aanzienlijk zal verbeteren.

Managementsamenvatting

- De Limburgse AI Chat Assistent (LAICA) is een AI-gestuurde chatbot ontwikkeld door het cluster Organisatie & Informatie (O&I) van de Provincie Limburg om ambtenaren te ondersteunen bij dagelijkse werkzaamheden. Het LAICA-project biedt een leveranciersonafhankelijke, modulaire, toekomstgericht, goedkoper en veiliger alternatief voor commerciële / openbare AI-chatbots, met naleving van privacywetgeving.

- De DPIA is uitgevoerd om de impact van het gebruik van LAICA op de bescherming van persoonsgegevens te beoordelen en potentiële privacy risico's te mitigeren. De DPIA identificeert vooral milde risico's, die adequaat worden aangepakt via voorzorgsmaatregelen door het hanteren van het privacy by design/default principe en training /bewustwording van gebruikers.

Belangrijkste Kenmerken van LAICA

- **Privacy gericht Ontwerp:** LAICA is ontwikkeld als een veiliger alternatief voor openbare AI-chatbots zoals ChatGPT. Het werkt binnen een afgeschermde omgeving, met nadruk op privacy by design en privacy by default.

- **Technische Componenten:** Entra ID (voorheen Azure AD) voor authenticatie, AI-taalmodellen via Azure (Microsoft) of VertexAI (Google), en een Virtual Machine waar de applicatie in draait en data wordt opgeslagen.

- **Gebruikersgegevens:** Gebruikers loggen in met naam, e-mailadres en wachtwoord. Gespreksgeschiedenis wordt lokaal in de browser van de gebruiker opgeslagen en beperkt toegankelijk tot de betreffende gebruiker.

- **Leveranciersonafhankelijkheid:** LAICA is modulair en flexibel ontworpen, met de intentie om toekomstige platformmigraties (bijv. naar Europese / Nederlandse alternatieven) mogelijk te maken.

Doel en Rechtsgrond

- **Doeleinden gegevensverwerkingen:** Persoonsgegevens worden verwerkt voor het aanbieden van diensten zoals authenticatie, het opslaan van gespreksgeschiedenis, en het verwerken van gebruikersinput.

- **Rechtsgrond:** De gegevensverwerking is gebaseerd op het gerechtvaardigd belang van de provincie om veilige en privacyvriendelijke tools te bieden, gezien de risico's van openbare AI-chatbots.

Beveiliging en Locaties

- **Beveiligingsmaatregelen:** Applicatie draait binnen een veilige virtual machine in de cloud, net als de taalmodellen, die uitsluitend benaderbaar zijn voor de beheerders. Inloggen op de applicatie kan uitsluitend via een provinciaal account. Binnen de applicatie wordt gebruik gemaakt van Role-based access control (RBAC) om rollen te beheren.

- **Risico-mitigatie:** Eindgebruikers worden actief geïnformeerd en getraind om geen gevoelige gegevens in te voeren. De systemen zijn niet gekoppeld aan andere databronnen en slaan geen persoonsgegevens centraal op.

Risicoanalyse

De belangrijkste geïdentificeerde risico's zijn:

1. **Onnodige verwerking van persoonsgegevens:** Gebruikers hebben de mogelijkheid onbedoeld meer persoonsgegevens in gesprekken in te voeren dan nodig. Dit wordt gemitigeerd door waarschuwingen en bewustwording.
2. **Afwezigheid van menselijke controle bij besluitvorming:** LAICA dient als advieshulpmiddel en geen vervanging voor menselijke kennis, wat expliciet aan gebruikers wordt gecommuniceerd.
3. **Misbruik bij exporteren van gesprekken:** Gebruikers kunnen gesprekken exporteren met mogelijk persoonsgegevens. Dit risico is hetzelfde als bij andere applicaties en wordt beperkt door trainingsinspanningen en technische maatregelen.

De risico's worden ingeschat als *laag* gezien de genomen maatregelen.

Om de privacy van betrokkenen te waarborgen, zijn onder andere de volgende maatregelen genomen:

- **Bewustwording:** Eindgebruikers ontvangen richtlijnen en trainingen over verantwoord gebruik van LAICA.
- **Masterprompt en waarschuwingen:** Bij invoer in LAICA worden gebruikers actief gewezen op het vermijden van gevoelige gegevens.
- **Richtlijnen:** Bij adviezen wordt expliciet aangegeven dat LAICA niet vervangt voor professioneel noodzakelijke kennis.

Functionaris Gegevensbescherming (FG) Advies

De uitgevoerde DPIA voldoet aan de criteria en er wordt positief op geadviseerd.

A. Beschrijving algemene kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Limburgse AI Chat Assistent (LAICA) V3

1. Voorstel

Beschrijf het voorstel waar de DPIA op toeziet op hoofdlijnen en benoem hoe het voorstel tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming van het voorstel.

Deze DPIA onderzoekt de gevolgen voor de bescherming van persoonsgegevens bij het gebruik van de Limburgse AI Chat Assistent (LAICA).

LAICA is een AI-gestuurde chatbot ontwikkeld voor en door de Provincie Limburg. De applicatie maakt gebruik van taalmodellen, zoals die van ChatGPT, maar is ontworpen met nadruk op privacy en informatieveiligheid, om risico's te minimaliseren.

Het voorstel waar deze DPIA op toeziet, is het ontwikkelen van LAICA als alternatief voor openbare AI-chatbots. Dit initiatief komt voort uit de wens om te experimenteren met verantwoorde toepassingen van AI-taalmodellen binnen de provinciale organisatie. Een experimenteergroep, opgericht door het cluster O&I van de Provincie Limburg, onderzoekt de mogelijkheden en risico's van deze technologieën. AI-taalmodellen kunnen een significante impact hebben op taken zoals beleidsanalyse, administratieve processen en het verbeteren van dienstverlening. Het is van belang om deze technologieën zorgvuldig te integreren, met oog voor zowel de voordelen als de privacy- en veiligheidseisen.

LAICA is een implementatie van het open source project GovChat-NL[1]. Deze implementatie bij de Provincie Limburg maakt gebruik van een Docker Image gehost in Elestio. Taalmodellen worden gehost in Microsoft Azure en Google Vertex AI. LAICA maakt momenteel gebruik van Open WebUI. Open WebUI is een self-hosted WebUI dat volledig offline opereert. Het ondersteunt verschillende LLM-runners, zoals Ollama en OpenAI-compatibele API's,. Open WebUI draait in VM-ware binnen een zelf gekozen cloudomgeving van Hetzner gevestigd binnen de EER (Neurenberg, D). De huidige versie van LAICA is gericht op tekstverwerking. Zie voor verder details de Documentatie Pilot-Implementatie Provincie Limburg.

Het gebruik van openbare chatbots, zoals ChatGPT, kan onwenselijk zijn vanwege de onduidelijkheid over wat er met de data gebeurt. Er ontbreken vaak contractuele afspraken, waardoor het onzeker is hoe en door wie de gegevens worden opgeslagen, verwerkt of gedeeld. Dit vormt een risico voor de privacy en voldoet mogelijk niet aan wet- en regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG). Daarom heeft de Provincie Limburg besloten om LAICA te ontwikkelen als een privacy-vriendelijker alternatief. Dit project is ontworpen met 'privacy by design' en 'privacy by default' principes. Technische en organisatorische maatregelen worden getroffen, zoals het gebruik van een afgeschermde Cloudomgeving en vooraf gedefinieerde richtlijnen voor de chatbot, om te waarborgen dat de assistent zich op een veilige en verantwoorde manier gedraagt.

[1] https://github.com/jeannotdamoiseaux/GovChat-NL

LAICA biedt dezelfde basisfunctionaliteiten als openbare chatbots, maar met minder risico's op het gebied van privacy en informatieveiligheid. In tegenstelling tot algemene publieke chatbots is LAICA ontworpen om binnen de grenzen van de privacywetgeving te opereren, zodat de Provincie Limburg haar medewerkers een veilige tool kan bieden voor dagelijkse werkzaamheden.

2. Persoonsgegevens

Beschrijf alle persoonsgegevens die worden verwerkt. Classificeer deze persoonsgegevens naar: gewoon, gevoelig, bijzonder, strafrechtelijk en wettelijk identificatienummer. Geef per categorie persoonsgegevens aan welke persoonsgegevens worden verzameld en geef aan wat de bron is van deze persoonsgegevens.

Categorie betrokkenen	Categorie persoonsgegevens	Persoonsgegevens	Type persoons-gegeven (gewoon, gevoelig, bijzonder, strafrechtelijk, identificatie-nummer)	Bron
Gebruikers	Basis identificatiegegevens	Naam	gewoon	AAD / Entra ID
Gebruikers	Basis identificatiegegevens	Emailadres	gewoon	AAD / Entra ID
Gebruikers	Basis identificatiegegevens	Gebruikersnaam/ wachtwoord	gevoelig	Direct van betrokkene
Gebruikers	Basis identificatiegegevens	User-id	gewoon	AAD / Entra ID
Gebruikers	Gebruikersinput	De gebruiker is in staat om tijdens het gesprek andere persoonsgegevens in te voeren. De gebruiker wordt er actief op gewezen dat dit niet de bedoeling is	gewoon	Direct van betrokkene en uit ingevoerde documenten

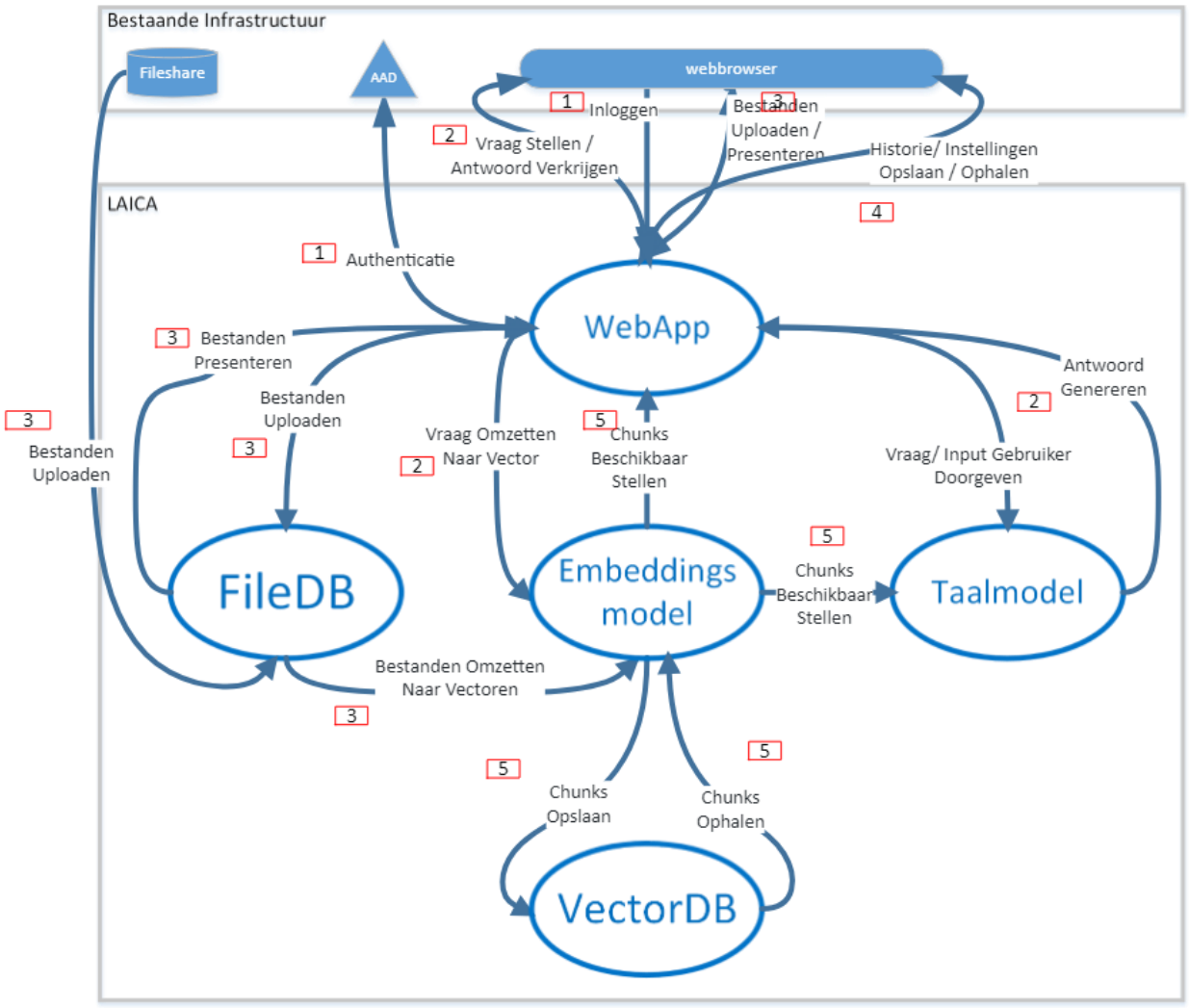
3. Gegevensverwerkingen

Geef alle gegevensverwerkingen weer en geef aan welke categorieën persoonsgegevens worden verwerkt per gegevensverwerking. Desgewenst kan een stroomschema van de gegevensverwerkingen worden toegevoegd.

	Gegevensverwerking	Categorieën persoonsgegevens
1	Authenticatie / autorisatie	Basis identificatiegegevens
2	Gebruikersinput verzenden / verwerken	Gebruikersinput / Basis identificatiegegevens
3	Bestanden uploaden / verwerken / presenteren	Gebruikersinput / Basis identificatiegegevens
4	Historie opslaan / ophalen	Gebruikersinput / Basis identificatiegegevens
5	Chunks opslaan / ophalen	Gebruikersinput

Gesprekshistorie wordt lokaal opgeslagen in de browser.

Om de eindgebruiker te autoriseren en te authentiseren, gebruiken we e-mailadres en wachtwoord. In de toekomst met MFA.



Voorbeeld van een afbeelding dat de samenhang tussen gegevensverwerkingen laat zien.

Globale werking LAICA:

1) inloggen met AAD / EntraID
2) Vraag stellen / beantwoorden
3) Bestanden uploaden / presenteren
4) Historie opslaan weergeven
5) Verwerking van de chunks

4. Technieken en methoden van de gegevensverwerkingen

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem, bijvoorbeeld, of sprake is van bijvoorbeeld (semi-) geautomatiseerde besluitvorming, profilering, een cloudoplossing of big data-verwerkingen en, zo ja, beschrijf waaruit dat bestaat.

LAICA bestaat uit drie hoofdbestanddelen: de inlogmethode (Entra ID), de applicatie inclusief chat- en documentopslag (VM in de cloud), en de embeddings- en taalmodellen (Microsoft Azure en VertexAI). Hieronder volgt een toelichting op de verschillende onderdelen:

Inlogmethode: Entra ID (voorheen Azure AD)

LAICA maakt gebruik van Entra ID (voorheen Azure Active Directory) om gebruikers te authenticeren en autoriseren. Dit zorgt ervoor dat alleen bevoegde gebruikers toegang hebben tot het systeem. De client- en serverzijde zijn afzonderlijk geregistreerd als aparte applicaties, elk met specifieke toegangsrechten.

Applicatie met webinterface (Open WebUI via Elestio)

De webinterface biedt een gebruikersvriendelijke omgeving waarin gebruikers eenvoudig kunnen inloggen, gesprekken voeren en bestanden uploaden. Geüploade bestanden kunnen tijdens het huidige gesprek worden bevraagd. Daarnaast kunnen gebruikers instellingen aanpassen om de zoekresultaten te beïnvloeden en gesprekken handmatig verwijderen indien gewenst.

Opslagstructuur:

- Bestandsopslag: Binnen de virtuele machine (VM) is een afzonderlijke map aanwezig voor geüploade bestanden. Wanneer een bestand wordt geüpload via de webinterface, wordt de inhoud van dat bestand omgezet in vectoren, oftewel wiskundige representaties van de tekst. Dit maakt het mogelijk om snel relevante informatie op te halen. Vragen van gebruikers worden eveneens omgezet in vectoren, waarna de meest relevante fragmenten in het bestand worden geïdentificeerd en gekoppeld aan de vraag. Deze fragmenten worden vervolgens toegevoegd als context bij de interactie in het gesprek. De bijbehorende vectoren en een SQL-databasebestand (.db) worden eveneens in deze VM omgeving opgeslagen.
- Gesprekken: De SQL-database wordt gebruikt om chatgesprekken op te slaan. Hierdoor is het mogelijk om bepaalde gesprekken later nog in te zien of te beheren. Voor de verwerking worden gesprekken lokaal in de browser van de gebruiker opgeslagen, niet in een gedeelde centrale database.

Taalmodellen (Microsoft Azure OpenAI en VertexAI) en embeddingsmodel

LAICA maakt gebruik van geavanceerde taalmodellen zoals OpenAI's GPT-3.5, GPT-4 en GPT-4o, evenals Claude 3.5 Sonnet van VertexAI. Deze modellen worden aangestuurd via de Azure OpenAI en VertexAI API's en draaien binnen een afgeschermde omgeving die exclusief beschikbaar is voor LAICA.

De taalmodellen zijn 'stateless', wat inhoudt dat ze geen gegevens onthouden en elke nieuwe vraag behandelen alsof het de eerste keer is. Ze leren niet van eerdere interacties en slaan geen communicatie permanent op. Door reeds gestelde vragen, antwoorden en relevante tekstfragmenten uit bestanden onzichtbaar toe te voegen aan nieuwe vragen, wordt echter context aangeboden aan het model. Dit resulteert in een meer interactieve en contextuele ervaring voor de gebruikers.

Een embeddingsmodel in de AI-architectuur zet woorden, zinnen of documenten om in numerieke representaties (vectoren). Deze representaties vangen de semantische betekenis van de tekst. In het geval van LAICA wordt dit gebruikt om gebruikersvragen te vergelijken met teksten en gegevens, wat het genereren van passende antwoorden mogelijk maakt.

Gegevensverwerking en gebruik

Bij het gebruik van LAICA is geen sprake van (semi-)geautomatiseerde besluitvorming of profilering. Het systeem is volledig gericht op het bieden van een efficiënte en effectieve ondersteuning voor de gebruiker. De cloudoplossing is ontworpen om de werking van LAICA te optimaliseren en de verwerking van big data te faciliteren.

5. Verwerkingsdoeleinden

Beschrijf de doeleinden van alle gegevensverwerkingen.

	Gegevensverwerking	Verwerkingsdoeleinde	Oorspronkelijk verwerkingsdoeleinde
1	Authenticatie / autorisatie naam, e-mailadres, wachtwoord, IP-adres	identificatie en authenticatie. noodzakelijk voor communicatie met betrokkene.	n.v.t.
2	Gebruikersinput verzenden / verwerken	Input van de gebruiker is noodzakelijk om gesprek te beginnen met een vraag	n.v.t.
3	Bestanden uploaden / verwerken / presenteren	Input van de gebruiker is noodzakelijk om context te schetsen en bronvermelding te genereren	n.v.t.
4	Historie opslaan / ophalen	Service aan de gebruiker	n.v.t.
5	Chunks opslaan / ophalen	Noodzakelijk om nauwkeurigheid en relevantie van de antwoorden te verbeteren	n.v.t.

Het initiatief tot de ontwikkeling van LAICA leidt tot een veiliger alternatief voor de commerciële taalmodellen welke aanzienlijke risico's met zich meebrengen inzake persoonsgegevens en bedrijfsgevoelige informatie.

Het gebruik van naam, e-mailadres en wachtwoord is nodig om gebruikers te verifiëren en authentiseren. Middels deze gegevens is het mogelijk om gebruikers toegang te geven tot hun eigen gesprekken die vastliggen in SQL-database (de tweede kolom in het bovenstaande procesdiagram).

Het IP-adres is in het kader van communicatie tussen server en cliënt ook benodigd.

6. Betrokken partijen

Benoem alle partijen die betrokken zijn en deel deze in per gegevensverwerking. Deel deze partijen in onder de rollen: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker, ontvanger, betrokkene(n) en derde. Wanneer bekend, benoem ook welke functionarissen/afdelingen binnen deze partijen toegang krijgen tot welke categorieën persoonsgegevens. Voeg aanvullende informatie toe in het tekstveld.

Naam partij	Rol partij	Functies/afdelingen	Persoonsgegevens
Provincie Limburg	Verwerkings-verantwoordelijke	I-Services / GM	naam, e-mailadres, wachtwoord,
Microsoft	Verwerker	n.v.t.	naam, e-mailadres, wachtwoord, gebruikersinput

De gebruiker kan tijdens het gesprek persoonsgegevens invoeren. Deze gegevens blijven binnen de afgeschermde omgeving. De AI-modellen hebben geen langetermijngeheugen en worden bij elke interactie opnieuw benaderd alsof het de eerste keer is. Ze leren niet van eerdere gesprekken met eindgebruikers

7. Belangen bij de gegevensverwerkingen

Beschrijf alle belangen die de betrokken partijen hebben bij de gegevensverwerkingen. Vraag betrokkenen of hun vertegenwoordigers ook naar hun mening over de verwerking indien relevant. Licht deze mening toe onder het belang van de betrokkenen.

Betrokken Partij	Belangen
Provincie Limburg / medewerker	Functioneel
O&I	Beheer / continuïteit
Microsoft	Bieden van diensten

De medewerker kan op vrijwillige basis gebruikmaken van LAICA. Daarnaast zijn de benodigde persoonsgegevens welke autorisatie en authenticatie mogelijk maken dezelfde persoonsgegevens die al gebruikt worden voor het gebruik van andere aan Entra ID (voorheen Azure AD) gekoppelde services welke de werknemer gebruikt of kan gebruiken. Als je gebruik wil maken van een taalmodel is dit de minst belastende manier. Immers bij gebruik van een commercieel taalmodel wordt het taalmodel met de persoonsgegevens van de betrokkene getraind.

De betrokkenen zullen over het algemeen onderdeel uit maken van de groep gebruikers van LAICA. Gebruikers worden bij het gebruik van LAICA erop gewezen om voorzichtig te zijn met persoonsgegevens. Bij het wijzen erop wordt doorgelinkt naar een Intranet-pagina met nadere uitleg. Verder wordt er middels interne bedrijfsinformatie en bewustwording gewezen op de wijze van gebruik van LAICA en met welke risico’s zij rekening dienen te houden. In die hoedanigheid zijn de gebruikers in hoge mate bewust en verwachten zij de verwerking. Wel leven er zorgen omdat het hier een nieuwe technologie betreft. Gedetailleerde ondersteuning en bewustwording blijft daarom een voorwaarde voor het verantwoordelijk gebruik van LAICA.

8. Verwerkingslocaties

Benoem in welke landen de gegevensverwerkingen plaatsvinden. Beschrijf het doorgiftemechanisme dat van toepassing is wanneer verwerkingslocaties buiten de Europese Economische Ruimte bevinden en noem of en welke aanvullende maatregelen van toepassing zijn. Voeg aanvullende informatie toe in het tekstveld.

Zie deel III van het Rijksmodel DPIA voor meer informatie over de doorgiftemechanismen.

	Gegevensverwerking	Verwerkingslocaties	Doorgiftemechanisme	Maatregelen
1	Authenticatie / autorisatie	Binnen EER	n.v.t.	n.v.t.
2	Gebruikersinput verzenden / verwerken	Binnen EER	n.v.t.	n.v.t.
3	Bestanden uploaden / verwerken / presenteren	Binnen EER	n.v.t.	n.v.t.
4	Historie opslaan / ophalen	Binnen EER	n.v.t.	n.v.t.
5	Chunks opslaan / ophalen	Binnen EER	n.v.t.	n.v.t.

Voor LAICA is ingesteld dat alle verwerkingslocaties binnen de EER zijn gekozen, Wij hebben bewust gekozen voor dataopslag binnen de Europese Economische Ruimte (EER). Het betreft een Europese hostingpartij Hetzner[2], met als data-locatie Neurenberg (Duitsland). Dit minimaliseert risico's rond data-export buiten de EU. Voor internationale gegevensoverdracht worden Standard Contractual Clauses (SCC's) gebruikt, passend bij de GDPR.

Sub verwerkers van Elestio zoals Hetzner hebben volgens de Data Processing Agreement (DPA) van Elestio[3] fysieke toegang tot de hardware van cloud providers, maar geen "logical" toegang. Met "logical" toegang wordt over het algemeen bedoeld dat zij geen directe toegang hebben tot de data die is opgeslagen op het systeem (bijvoorbeeld geen inloggegevens of systemen waarmee ze de inhoud van de data kunnen inzien of wijzigen). Hierdoor kunnen deze partijen technisch gezien niet bij de persoonsgegevens, zelfs al beheren of onderhouden zij de fysieke servers waarop de data draait. Dit is een veiligheidsmaatregel om persoonsgegevens te beschermen en te voldoen aan vereisten zoals de AVG.

Elestio implementeert en onderhoudt Specifieke technische en organisatorische veiligheidsmaatregelen zoals:Gegevens worden versleuteld bij opslag (at rest) en tijdens overdracht (in transit) met AES-256 en TLS 1.2/1.3. Servers worden gehost in datacenters met certificeringen zoals ISO 27001 en SOC 2. Toegang tot deze datacenters is beperkt tot geautoriseerde personen. Alle toegang tot persoonsgegevens wordt geregistreerd, en deze logs worden minimaal 12 maanden bewaard. Er is een formeel incident-responsplan in geval van een datalek, inclusief detectie, mitigatie en rapportage binnen 48 uur.

LAICA maakt gebruik van Entra ID van Microsoft (voorheen Azure Active Directory) om gebruikers te authentiseren en autoriseren. Dit zorgt ervoor dat alleen bevoegde gebruikers toegang hebben tot het systeem. Om LAICA te laten functioneren, maken we verder gebruik van AI-taalmodellen die aangeboden worden vanuit Azure OpenAI. Uit de tussen de Provincie Limburg en Microsoft gesloten Enterprise Agreement volgt dat iedere doorgifte van persoonsgegevens buiten de EER in het kader van de overeenkomst wordt beheerst door de modelcontractbepalingen die door Microsoft zijn opgesteld en

[2] https://www.hetzner.com/legal/terms-and-conditions/
[3] https://docs.elest.io/books/legal-compliance/page/elestio-data-processing-agreement

gepubliceerd als de Bijlage bescherming van persoonsgegevens voor Producten en Diensten. De Enterprise Agreement stelt dat, indien de modelcontractbepalingen niet langer van toepassing of beschikbaar zijn, Microsoft garandeert dat er een andere passende waarborg voor de doorgifte van persoonsgegevens kan worden aangewezen. Mocht blijken dat de doorgifte van persoonsgegevens desondanks of bij het ontbreken van een passende waarborg niet rechtmatig is, dan geeft de Enterprise Agreement Provincie Limburg de bevoegdheid om het gebruik van Microsoft Entra ID (voorheen Azure AD) met onmiddellijke ingang te beëindigen.

9. Juridisch en beleidsmatig kader

Benoem alle wet- en regelgeving en beleid met mogelijke gevolgen voor de gegevensverwerkingen. De AVG en de Richtlijn[4] hoeven niet genoemd te worden. Voeg aanvullende informatie toe in het tekstveld.

	Gegevensverwerking	Gegevens-verwerkingen	Juridisch en/of beleidsmatig kader	Wetsartikelen
1	Authenticatie / autorisatie aanvraag		• ***BIO (2.0) en NIS2 (Cbw)***	
2	Gebruikersinput verzenden / verwerken		• ***BIO (2.0) en NIS2 (Cbw)*** • ***Ambtenarenwet 2017*** • ***Gedragscode Ambtelijke Integriteit*** • ***AI-verordening***	
3	Bestanden uploaden / verwerken / presenteren		• ***BIO (2.0) en NIS2 (Cbw)*** • ***Ambtenarenwet 2017*** • ***Gedragscode Ambtelijke Integriteit*** • ***AI-verordening***	
4	Historie opslaan / ophalen		• ***BIO (2.0) en NIS2 (Cbw)*** • ***AI-verordening***	
5	Chunks opslaan / ophalen		• ***BIO (2.0) en NIS2 (Cbw)*** • ***AI-verordening***	

Naast de AVG is de volgende wetgeving van kracht óf zal de volgende wetgeving van kracht worden:

• ***Baseline Informatieveiligheid Overheid (2.0) en NIS2 (Cbw) (1-5)***

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen.

• ***Ambtenarenwet 2017 (2-3)***

[4] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Artikel 9: “De ambtenaar en de gewezen ambtenaar zijn verplicht tot geheimhouding van hetgeen hen in verband met hun functie ter kennis is gekomen, voor zover die verplichting uit de aard der zaak volgt.” Dit betekent dat het gebruik van LAICA een voorziening moet hebben om met geheimhouding om te gaan.

• ***Gedragscode Ambtelijke Integriteit (2-3)***

Artikel 2.2: vertrouwelijk omgaan met gevoelige informatie. LAICA draagt als privacy vriendelijk alternatief voor o.a. ChatGPT bij aan de naleving van dit artikel.

• ***AI-verordening (1-5)***

De AI-verordening is een Europese wet die regels stelt voor de ontwikkeling en het gebruik van AI-systemen. Ook geeft de wet rechten aan burgers die in aanraking komen met AI-systemen. Het doel van de wet is dat AI-systemen die organisaties (binnen de EU) gebruiken, veilig zijn en fundamentele rechten respecteren. Het maakt niet uit of die AIsystemen binnen of buiten de EU zijn ontwikkeld. AI-systemen worden onderverdeeld in verschillende risicocategorieën. Afhankelijk van de categorie waarin een AI-systeem valt, gelden zwaardere, minder zware of geen regels.

10. Bewaartermijnen

Bepaal de bewaartermijnen van de persoonsgegevens aan de hand van de gegevensverwerkingen en de verwerkingsdoeleinden. Motiveer waarom deze bewaartermijnen niet langer zijn dan strikt noodzakelijk ten opzichte van de verwerkingsdoeleinden. Beschrijf wie toeziet op de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn. Voeg aanvullende informatie toe in het tekstveld.

	Gegevensverwerking	Verwerkings-doeleinde	Categorie Persoons-gegevens	Bewaartermijn	Motivatie bewaar-termijn
1	Authenticatie / autorisatie aanvraag	identificatie en authenticatie. noodzakelijk voor communicatie met betrokkene.	contactgegevens	Duur dienstverband	Centraal beleid
2	Gebruikersinput verzenden / verwerken	Input van de gebruiker is noodzakelijk om gesprek te beginnen met een vraag	Gebruikersinput / contactgegevens	Één maand	Gebruikers kunnen dit zelf verwijderen
3	Bestanden uploaden / verwerken / presenteren	Input van de gebruiker is noodzakelijk om context te schetsen en bronvermelding te genereren	Gebruikersinput / contactgegevens	Individueel: Maand Documenten blijven in de centrale kennisbank totdat deze niet meer actueel zijn	Gebruikers kunnen deze zelf verwijderen Beheer gedreven

	Gegevensverwerking	Verwerkings-doeleinde	Categorie Persoons-gegevens	Bewaartermijn	Motivatie bewaar-termijn
4	Historie opslaan / ophalen	Service aan de gebruiker	Gebruikersinput / contactgegevens	Één maand	Gebruikers kunnen dit zelf verwijderen
5	Chunks opslaan / ophalen	Noodzakelijk om nauwkeurigheid en relevantie van de antwoorden te verbeteren	Gebruikersinput	Chunks blijven in de centrale kennisbank totdat deze niet meer actueel zijn	Beheer gedreven

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen en rechten van de betrokkene.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd. Iedere rechtsgrond moet aan bepaalde voorwaarden voldoen, voeg in de toelichting op de rechtsgrond toe hoe aan deze voorwaarden wordt voldaan. Voeg aanvullende informatie toe in het tekstveld.

	Gegevensverwerking	Rechtsgrond	Toelichting op de rechtsgrond
1	Authenticatie / autorisatie aanvraag	Noodzakelijk voor de behartiging van een gerechtvaardigd belang	Het is een feit van algemene bekendheid dat medewerkers gebruikmaken van ChatGPT of andere openbare Chatbots voor hun werkzaamheden. Daarmee worden de belangen van de organisatie op het gebied van privacy en informatieveiligheid geschaad. Ook worden de individuele privacybelangen van gebruikers geschaad. Om deze belangen beter te waarborgen heeft de provincie LAICA ontwikkeld.
2	Gebruikersinput verzenden / verwerken	Noodzakelijk voor de behartiging van een gerechtvaardigd belang	‘’
3	Bestanden uploaden / verwerken / presenteren	Noodzakelijk voor de behartiging van een gerechtvaardigd belang	‘’
4	Historie opslaan / ophalen	Noodzakelijk voor de behartiging van een gerechtvaardigd belang	‘’
5	Chunks opslaan / ophalen	Noodzakelijk voor de behartiging van een gerechtvaardigd belang	‘’

12. Bijzondere persoonsgegevens

Het verwerken van bijzondere of strafrechtelijke persoonsgegevens is in principe verboden. Verwerking is pas mogelijk wanneer een uitzonderingsgrond van toepassing is. Beoordeel of een van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een nationaal identificatienummer, beoordeel of dit is toegestaan.

	Gegevensverwerking	Type bijzonder persoonsgegeven	Uitzonderingsgrond
2	Gebruikersinput verzenden / verwerken	Gebruiker kan bijzondere persoonsgegevens verzenden. Dit wordt afgeraden in de instructie.	

13. Doelbinding

Als de persoonsgegevens voor een ander doeleinde worden verwerkt dan het doeleinde waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, beoordeel of deze (nieuwe) verdere verwerking toelaatbaar is op grond van Unie- of lidstaatrechtelijk recht, dan wel verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Voeg in het tekstveld de verenigbaarheidstoets en aanvullende informatie toe.

	Gegevensverwerking	Persoonsgegevens	Doeleinde	Oorspronkelijk doeleinde
n.v.t.				

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk en evenredig zijn voor het verwezenlijken van de verwerkingsdoeleinden.

Ga hierbij in ieder geval in op:

a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?

- Ja, er worden er niet meer persoonsgegevens verwerkt dan strikt noodzakelijk voor de doeleinden

b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?

- Nee, want de andere wijze is ChatGPT. LAICA is juist ontwikkeld om de medewerkers toegang te verlenen tot een tool die veiliger is en waar minimale persoonsgegevens worden verwerkt.

15. Rechten van betrokkenen

Beschrijf de procedure waarmee invulling wordt gegeven aan de rechten van de betrokkenen Als de rechten van de betrokkene worden beperkt, beschrijf op grond van welke wettelijke uitzondering dat is toegestaan.

Rechten van betrokkene	Procedure ter uitvoering	Beperking op grond van wettelijke uitzondering
Recht van inzage	Handleiding Rechten van betrokkenen	
Recht op rectificatie en aanvulling	Handleiding Rechten van betrokkenen	
Recht op vergetelheid	Handleiding Rechten van betrokkenen	
Recht op beperking van de verwerking	Handleiding Rechten van betrokkenen	
Recht op dataportabiliteit	Handleiding Rechten van betrokkenen	
Recht niet onderworpen te worden aan geautomatiseerde besluitvorming	Handleiding Rechten van betrokkenen	
Recht om bezwaar te maken	Handleiding Rechten van betrokkenen	
Recht op duidelijke informatie	Handleiding Rechten van betrokkenen	

Maandelijks worden bestanden en historie verwijderd. Op aanvraag kunnen alle gegevens worden verwijderd

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerkingen.

16. Risico's voor betrokkenen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

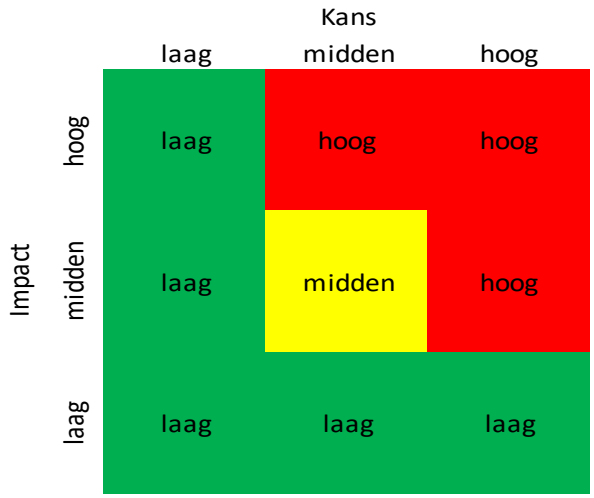
a. *welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;*

b. *de oorsprong van deze gevolgen;*

c. *de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;*

d. *de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.*

Gebruik voor de inschatting van de kans, impact en het risico de niveaus 'laag', 'gemiddeld' en 'hoog'. De kans wordt bepaald aan de hand van de formule kans x impact. Gebruikmaken van de bijbehorende kleuren is aan te raden. De onderstaande matrix kan worden gebruikt voor het vaststellen van de risico's voor betrokkenen.



**De bovenstaande risicomatrix is illustratief. Risico's met een lage impact of lage kans worden als laag ingeschat indien het risico niet verder kan worden gemitigeerd. Zo kan bijvoorbeeld de impact van ransomware hoog zijn, maar door het nemen van de juiste technische maatregelen de kans (zeer) laag. Het risico kan dan ten behoeve van de risico-acceptatie als laag beschouwd worden.*

	Beschrijving risico	Kans	Impact	Risico-inschatting
1	Er worden meer persoonsgegevens gebruikt dan noodzakelijk	Midden, eindgebruikers zijn volledig vrij om	Laag, want de gesprekken worden op een	Laag

	Beschrijving risico	Kans	Impact	Risico-inschatting
	Vrije tekstvelden vullen met niet noodzakelijke (mogelijk zelfs gevoelige of bijzondere) persoonsgegevens. Meer gegevens verwerken dan noodzakelijk voor het bereiken van het doel. Eindgebruikers hebben de mogelijkheid om persoonsgegevens te verwerken in de gesprekken die ze voeren met de chatbot.	persoonsgegevens in de gesprekken te gebruiken. Er wordt bij de invoer van tekst echter gewezen op het voorzichtig omgaan met persoonsgegevens in gesprekken.	veilige manier binnen onze eigen VM SQL-database opgeslagen en na één maand verwijderd. De gesprekken zijn daarnaast alleen toegankelijk voor de gebruiker die het gesprek voert.	
2	Als er sprake van geautomatiseerde individuele besluitvorming wordt de menselijke controle verzuimd. Eindgebruikers kunnen LAICA om advies vragen over een onderwerp. Dit advies kan als basis dienen voor een besluit dat door de eindgebruiker genomen wordt. Dit besluit heeft nog geen rechtsgevolg als het niet door het besluitvormingsproces heeft doorlopen.	Laag, want bij het voeren van een gesprek wordt een eindgebruiker actief gewezen op het feit dat LAICA geen vervanging is voor professionele kennis en slechts dient als hulpmiddel.	Midden, LAICA is niet gekoppeld aan andere systemen.	Laag
3	LAICA biedt de mogelijkheid om gesprekken te exporteren. De gebruiker kan zijn/haar gesprekstekst in een tekstdocument exporteren. Na het exporteren heeft de provincie geen zicht meer op de daarin opgenomen data. Dit is echter niet anders dan in iedere andere applicatie die de provincie ter beschikking stelt aan medewerkers.	Laag, want LAICA is niet ontworpen om persoonsgegevens van andere betrokkenen dan de betreffende medewerker te verwerken. Het risico doet zich louter voor als een medewerker ten eerste moedwillig persoonsgegevens van andere invoert en die buiten het systeem exporteert. Zoals eerder benoemd is dit niet anders dan bij iedere andere applicatie.	Midden, het betreft voornamelijk de persoonsgegevens van betrokkenen zelf. Afhankelijk van wat de medewerker in het vrije tekstveld invoert.	Laag

D. Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen.

Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de DPIA is in het bijzonder expertise over informatiebeveiliging belangrijk.

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt. Voeg aanvullende informatie in het tekstveld onder de tabellen toe.

Beschrijf ook de resterende risico's die nog aanwezig zijn na de uitvoering en/of implementatie van de geïdentificeerde maatregelen. Geef per resterend risico aan wat het niveau is van dit risico.

Geef tot slot een conclusie over de restrisico's. Zijn deze acceptabel? En is er een voorafgaande raadpleging bij de Autoriteit Persoonsgegevens nodig?

Gebruik voor de inschattingen van de risico's de niveaus 'laag', 'gemiddeld' en 'hoog'. Gebruikmaken van de bijbehorende kleuren is aan te raden.

	Risico	Maatregelen	Resterend risico en risico-inschatting	Beheerder van maatregelen
1	Er worden meer persoonsgegevens gebruikt dan noodzakelijk Vrije tekstvelden vullen met niet noodzakelijke (mogelijk zelfs gevoelige of bijzondere) persoonsgegevens. Meer gegevens verwerken dan noodzakelijk voor het bereiken van het doel.	Er wordt bij de invoer van tekst gewezen op het voorzichtig omgaan met persoonsgegevens in gesprekken. Masterprompt is zodanig opgesteld dat de gebruiker erop wordt gewezen voorzichtig om te gaan met persoonsgegevens zodra deze worden gedetecteerd in de prompt Eindgebruikers er actief op wijzen middels richtlijnen, bewustwording en training om geen persoonsgegevens te delen. LAICA is ontworpen om persoonsgegevens veilig op te slaan. Ook hier is van toepassing dat	Laag	Provincie Limburg

	Risico	Maatregelen	Resterend risico en risico-inschatting	Beheerder van maatregelen
		persoonsgegevens niet verder gedeeld worden met andere partijen, zoals OpenAI of Microsoft.		
2	Als er sprake van geautomatiseerde individuele besluitvorming wordt de menselijke controle verzuimd.	Bij het voeren van een gesprek wordt een eindgebruiker actief gewezen op het feit dat LAICA geen vervanging is voor professionele kennis en slechts dient als hulpmiddel. LAICA is niet gekoppeld aan andere systemen. Medewerkers blijven wijzen middels richtlijnen, bewustwording en training op het feit dat LAICA een hulpmiddel is en dat alle antwoorden die gegenereerd worden, dienen te worden gecontroleerd. Tekst in webapp: “LAICA kan fouten maken. Controleer belangrijke informatie.”	Laag	Provincie Limburg
3	Door afwijkende activiteiten met persoonsgegevens worden er meer persoonsgegevens opgeslagen, persoonsgegevens gedeeld, persoonsgegevens opgeslagen op niet daarvoor bedoelde plekken.	LAICA is niet ontworpen om persoonsgegevens van andere betrokkenen dan de betreffende medewerker te verwerken. Het risico doet zich louter voor als een medewerker, al dan niet moedwillig, persoonsgegevens invoert en de in/output buiten het systeem exporteert. Gesprekshistorie wordt op een veilige manier binnen onze eigen VM SQL-database opgeslagen en na één maand verwijderd. De gesprekken zijn standaard alleen toegankelijk voor de applicatiebeheerder en de gebruiker die het gesprek voert. Gebruikers kunnen daarnaast een tijdelijke chat	Laag	Provincie Limburg

	Risico	Maatregelen	Resterend risico en risico-inschatting	Beheerder van maatregelen
		starten waarbij de gesprekshistorie niet wordt opgeslagen. Applicatie draait binnen een veilige virtual machine in de cloud, net als de taalmodellen, die uitsluitend benaderbaar zijn voor de beheerder. Inloggen op de applicatie kan uitsluitend via een provinciaal account. Binnen de applicatie wordt gebruik gemaakt van Role-based access control (RBAC) om rollen en toegang te beheren. Medewerkers blijven wijzen middels richtlijnen, bewustwording en training op het verantwoord omgaan met persoonsgegevens en gesprekken ook na het maken van een export. Data na contractbeëindiging: Indien het contract wordt beëindigd, hebben we 90 dagen de tijd om onze (persoons)gegevens veilig te stellen. Dit proces moeten we zelf organiseren.		

Algemeen advies is om ervoor te zorgen dat bovenstaande maatregelen toekomstbestendig blijven d.m.v. het organiseren van beheer (beheerorganisatie) en monitoring op Laica.

18. Advies Functionaris Gegevensbescherming

FG-advies over de DPIA RX LAICA[5]

Op grond van artikel 35 lid 2 AVG brengt de FG advies uit op een door de verwerkersverantwoordelijke uitgevoerde DPIA. Hiervoor heeft de provincie ook een eigen uitvoeringsprotocol opgesteld.

Samengevat voldoet de uitgevoerde DPIA aan de criteria en geef ik een positief advies.

[5] DOS-00073322

Uitwerking

Een DPIA mag altijd worden uitgevoerd en is voor sommige (voorgenomen) verwerkingen van persoonsgegevens verplicht. Het is terecht dat een DPIA is uitgevoerd, met name vanwege de nieuwe technologie die wordt ingezet bij de (mogelijke) verwerking van persoonsgegevens. De Autoriteit Persoonsgegevens noemt dit een van de criteria[6] om een DPIA uit te voeren.

In de DPIA wordt aangegeven:

Het gebruik van openbare chatbots, zoals ChatGPT, kan onwenselijk zijn vanwege de onduidelijkheid over wat er met de data gebeurt. Er ontbreken vaak contractuele afspraken, waardoor het onzeker is hoe en door wie de gegevens worden opgeslagen, verwerkt of gedeeld. Dit vormt een risico voor de privacy en voldoet mogelijk niet aan wet- en regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG).

Ik wijs hier op de DPIA die door het Rijk is uitgevoerd op de risico's van het gebruik van de openbare versies van ChatGPT[7].

Goed om te lezen dat de Provincie onder andere vanwege de risico's van het gebruik van openbare versies van ChatGPT als beschermende maatregel kiest voor het ontwikkelen van een eigen chatbot.

Ik zal hierna aan de hand van de in de AVG verplichte onderdelen advies uitbrengen. Deze worden genoemd onder artikel 35 lid 7.

Norm	Aanwezig in DPIA	Advies
a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;	Hoofdstuk 1 - 10	De beschrijving geeft een compleet beeld van de doelen en welke gegevens precies worden verwerkt.
b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;	Hoofdstuk 11 - 14	De gegevens worden verwerkt op basis van een gerechtvaardigd belang.
c) een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen; en	Hoofdstuk 15 en 16	Besteed nog aandacht aan transparantie / voorlichting voor de gebruiker / betrokkene (Laica – info, ik zie dat het er is, maar wordt niet benoemd in de

[6] Data protection impact assessment (DPIA) | Autoriteit Persoonsgegevens onder punt 4

[7] https://slmmicrosoftrijk.nl/wp-content/uploads/2024/12/20241218-Public-version-DPIA-Microsoft-365-Copilot-for-SLM-Rijk.pdf.

		risico's). In hoofdstuk 17 komt dit wel mooi terug bij de maatregelen.
d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.	Hoofdstuk 17 + bijlage met overzicht	De risico's hebben een laag profiel waardoor er een planning met te nemen maatregelen ontbreekt. Neem daarom een datum op wanneer wordt gecontroleerd of de maatregelen genomen zijn. Verder is van belang om ieder half jaar (of naar wens eerder) deze DPIA te herzien. Het gaat namelijk om een lopend experiment. Als LAICA voor andere doelen wordt ingezet, bijvoorbeeld als het een onderdeel wordt van een proces, dan kan de grondslag en de gebruikte persoonsgegevens wijzigen.

Ondertekening
Om de DPIA formeel vast te stellen is het noodzakelijk deze te ondertekenen, zodat het duidelijk is dat de DPIA door de verantwoordelijke(n) akkoord is bevonden.

Naam verantwoordelijke(n)	[redacted]
Directie/afdeling verantwoordelijke(n)	
Functie verantwoordelijke(n)	
Datum ondertekening	
Handtekening	