# IMPACT ASSESSMENT MENSENRECHTEN EN ALGORITMES / DATA PROTECTION IMPACT ASSESSMENT CHATBOT MAI

| Functie | Naam |
|---|---|
| Projectleider | [redacted] |
| Proceseigenaar | [redacted] |
| Privacy Officer | [redacted] / [redacted] |
| Inkoop | |
| CISO | [redacted] |
| FG | [redacted] |

## A. Beschrijving kenmerken gegevensverwerkingen

### 1. Voorstel

| Wat wil je bereiken met het proces/project? Wat is het doel?<br>*[Geef aan welk(e) doel(en) de organisatie met de (nieuwe of gewijzigde) werkprocessen wil bereiken en/of binnen welk context deze gezien moeten worden.* |
|---|
| Mai is een chatbot die 24/7 algemene vragen van burgers beantwoordt op de website van gemeente Montferland. De chatbot vervangt de huidige livechat om wachttijden te verminderen en directe antwoorden te bieden.<br><br>IAMA: de chatbot maakt gebruik van een impactvol algoritme. In principe werkt de chatbot volledig zelfstandig; de chatbot maakt gebruik van de volgende gegevensbronnen: informatie van de gemeentelijke website, Algemene Plaatselijke Verordening (APV) en aanvullende documenten met gemeentelijke informatie.<br><br>In principe worden geen persoonsgegevens verwerkt; het kan echter zo zijn dat een bezoeker zijn naam en andere persoonsgegevens invoert (hoewel dit vooraf duidelijk wordt aangegeven niet te doen). Gebeurt het wel, dan moet de gemeente deze gegevens op gepaste wijze en in lijn met da AVG behandelen. |

### 2. Hoe werkt het precies?

| *Beschrijf het systeem, de applicaties, de in- en output, of er acties worden gedaan zonder tussenkomst/beoordeling van de mens (maak een plaatje van het proces).*<br>*Beschrijf ook alle gegevensverwerkingen (Een verwerking is alles wat je met persoonsgegevens kunt doen: verzamelen, vastleggen, opslaan, bijwerken of wijzigen, opvragen, raadplegen, versturen, combineren, afschermen, vernietigen etc).* |
|---|
| Mai is gebaseerd op een RAG-systeem (Retrieval-Augmented Generation) en maakt gebruik van de volgende componenten:<br>- Platform: Flowise (open-source, on-premises gehost)<br>- Vector Database: Qdrant (open-source, on-premises gehost)<br>- Large Language Model (LLM) en Embedding: Azure OpenAI deployments (eigen instantie). Dit systeem stelt de chatbot in staat om relevante informatie op te halen uit de beschikbare |

bronnen en deze te combineren met de capaciteiten van het taalmodel om accurate en contextrelevante antwoorden te genereren.

Alle systemen draaien on-premise en alle gegenereerde info blijft 'in house'.

## 2.1. Wat zijn de baten voor de gemeente Montferland als organisatie?

| *Bij baten kun je denken aan vrijheid, welzijn, welvaart, duurzaamheid, inclusiviteit en diversiteit, gelijkheid, efficiëntie en kostenreductie. (Deze brede benadering is belangrijk, omdat ethische en juridische aspecten invloed kunnen hebben op de relatie tussen onze organisatie en de omgeving)* |
|---|
| Door de inzet van de chatbot hebben onze KCC medewerkers meer tijd voor complexe zaken en zaken waarbij menselijk contact onontbeerlijk is. Er is sprake van verhoogde efficiëntie en kostenreductie op de lange termijn terwijl we tegelijkertijd de service aan onze inwoners verbeteren. |

## 2.2. Wat zijn de baten voor het individu?

| De inwoner wordt altijd meteen te woord gestaan bij een breed scala aan vragen, ook in de avonduren en tijdens de weekends. |
|---|

## 3. Persoonsgegevens

| Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Geef de categorieën een risicoklasse.<br>*Denk aan medewerkers, kinderen, cliënten, bezoekers of gebruikers. Denk bij persoonsgegevens bijvoorbeeld aan naam, adres, telefoonnummer, BSN, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, kenteken, bankrekeningnummer en -saldo, functie, opleiding, inkomens-en vermogensgegevens, lidmaatschap vakbond, persoonlijke voorkeuren, loonschaal, gespreksverslagen, gegevens over de gezondheid of strafrechtelijke gegevens (Denk bij risicoklasse I aan NAW, bij II aan bijzondere persoonsgegevens zoals ras, etniciteit en gezondheid en bij III aan strafrechtelijke gegevens).* |
|---|

| Persoon | Soort persoonsgegeven | Risico klasse |
|---|---|---|
| ***Opmerking: in principe worden géén persoonsgegevens verwerkt! Het kan echter voorkomen dat een bezoeker gegevens ingeeft. Wanneer dit gebeurt wordt daar op zorgvuldige wijze mee omgegaan en worden ze behandeld zoals hieronder is weergegeven.*** | | |
| Website bezoeker / chatbot gebruiker | (in voorkomend geval) naam en contactgegevens | I |
| Website bezoeker / chatbot gebruiker | Gevoelige persoonsgegevens (locatiegegevens, financiële gegevens, BSN) | II |
| Website bezoeker / chatbot gebruiker | Bijzondere persoonsgegevens (medische gegevens, ras, sexuele geaardheid, enz.) | II |

## 4. Gegevensverwerkingen

| Geef alle voorgenomen gegevensverwerkingen weer. (Deel het proces op in verschillende stappen) |
|---|
| Het bericht van de gebruiker wordt door de LLM geanalyseerd op intentie, daarna geoptimaliseerd voor vectorisatie t.b.v. similarity search in de relevante vector database(s), daarna wordt het oorspronkelijke bericht inclusief opgehaalde documenten gevoed aan een LLM die een antwoord formuleert. De gebruiker kan na ieder bericht ook nog feedback leveren in de vorm van een duimpje omhoog/omlaag en een vrije input. Dit alles wordt opgeslagen in een eigen SQLite databse. |

## 5. Verwerkingsdoeleinden

| Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen. |
|---|
| Het primaire doel is om een passend antwoord te kunnen formuleren voor de gebruiker. Het secundaire doel is verbetering van de chatbot op basis van de berichten en de eventuele feedback erop. |

## 6. Betrokken partijen

| Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens. |
|---|
| In principe zijn alleen website bezoekers en gebruikers van de chatbot en de gemeente ambtenaren betrokken partijen. De gemeente is verwerkingsverantwoordelijke in deze; er is geen sprake van een verwerker. Binnen de gemeente krijgen alleen de functionarissen, die belast zijn met het monitoren van de input. |

## 7. Belangen bij gegevensverwerkingen

| Beschrijf alle belangen die de verwerkingsverantwoordelijken en anderen hebben bij de voorgenomen gegevensverwerkingen. |
|---|
| Het primaire belang is verbeterde diensverlening voor de inwoners. Het secundaire belang is het verbeteren van de output van de chatbot. |

## 8. Technieken en methoden van de gegevensverwerking

| Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-) geautomatiseerde besluitvorming, profilering of big-data verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat. |
|---|
| Met eventuele persoonsgegevens wordt in principe niets gedaan. Wij werken momenteel aan een uitbreiding die automatisch een melding maakt in het geval dat een gebruiker toch persoonsgegevens deelt, welke wij dan permanent zullen verwijderen. |

## 9. Juridisch en beleidsmatig kader

| Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen. *Denk aan wetten, besluiten, gedragscodes, convenanten of beroepscodes. Ook normenkaders zoals ISO/NEN.* |
|---|
| Van toepassing zijnde wetgeving is o.a. de Gemeentewet en Algemene Plaatselijke Verordeningen, als ook besluiten om gebruik te maken van AI-toepassingen. |

| |
|---|
| Daarnaast is ook het informatiebeveiliging normenkader BIO (baseline informatiebeveiliging overheid) van toepassing. |

### 10. Bewaartermijnen

| |
|---|
| Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden. |
| Zoals al aangegeven worden in principe geen persoonsgegevens verwekt. In voorkomend geval, wanneer de gebruiker persoonsgegevens invult, worden deze z.s.m. verwijderd. E.e.a. volgens het gestelde in AVG, artikel 5 lid 1.e: *Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen („opslagbeperking").* |

## B. Beoordeling rechtmatigheid gegevensverwerkingen

*Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.*

### 1. Rechtsgrond

| |
|---|
| Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd. *Kies 1 uit de volgende opties : overeenkomst, wettelijke plicht, vitaal belang, toestemming, gerechtvaardigd belang, publieke taak.* |
| De rechtsgrond voor de verwerking is gelegen in AVG artikel 6 lid 1.e, het uitvoeren van een taak in het algemeen belang en/of het uitvoeren van het openbaar gezag, vastgelegd in o.a. de Gemeentewet. |

### 2. Bijzondere persoonsgegevens

| |
|---|
| Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan. |
| Er worden - in principe - geen bijzondere en of gevoelige persoonsgegevens verwerkt. Het kan echter voorkomen dat een bezoeker persoonsgegevens invoert. Deze worden dan z.s.m. gepseudonimiseerd/geanonimiseerd en zo spoedig mogelijk verwijderd. |

### 3. Doelbinding

| |
|---|
| Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.<br>*Gebruik je de persoonsgegevens die je voor dit proces of project hebt verzameld ook nog voor iets anders? Is deze verdere verwerking dan verenigbaar is met het doel waarvoor ze zijn verzameld? Denk bijvoorbeeld aan gegevens voor de zorgovereenkomst die vervolgens worden gebruikt voor een onderzoek.* |
| Gegevens worden alleen voor het doel waarvoor ze zijn verstrekt, verwerkt. Zoals al aangegeven gaat het niet om persoonsgegevens, maar om het verstrekken van algemene, gemeentelijke informatie. |

### 4. Noodzaak en evenredigheid

| |
|---|
| Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit. a) Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden? b) Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt? |
| Principes van noodzakelijkheid, evenredigheid, proportionaliteit en subsidiariteit worden strikt toegepast. In principe is het aanbieden van deze dienst de meest privacy vriendelijke wijze voor betrokkene (hij/zij blijft in principe volledig anoniem). |

### 5. Rechten van betrokkenen

| |
|---|
| **Wat zijn de (mogelijk) negatieve gevolgen voor de betrokkenen**<br>*Beschrijf en beoordeel risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen.* |

| Negatieve gevolgen | Oorzaak hiervan | Kans op gevolgen | Impact van gevolgen |
|---|---|---|---|
| Niet (tijdig) verwijderen van persoonsgegevens | Menselijk handelen | Verwaarloosbaar/nihil | verwaarloosbaar |

## C. Beschrijf en beoordeel de risico's van de gegevensverwerkingen

### 1. Risico's

*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; 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.*

| Nr. | Risico | Oorsprong | Gevolg | Kans | Impact |
|---|---|---|---|---|---|
| 1 | Niet (tijdig) verwijderen van persoonsgegevens | Menselijk handelen | Verwaarloosbaar/nihil | verwaarloosbaar | verwaarloosbaar |

# D. Voorgenomen maatregelen

*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 PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.*

## 1. 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 en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is. |

| Nr. Risico | Risico | Maatregelen ISO | ISO of NEN norm | Restrisico |
|---|---|---|---|---|
| 1 | Niet (tijdig) verwijderen van persoonsgegevens | - Datawiping c.q. vernietiging<br>- Opstellen procedure vernietiging<br>- Uitvoeren toezicht en controle<br>- Opstellen beleid voor verwijderen van gegevens. | ISO 27001 en BIO 6.2.3 gegevens verwijdering na bewaartermijn en 10.7.1 beheer van verwijderde gegevens | verwaarloosbaar |

## 2. Transparantie

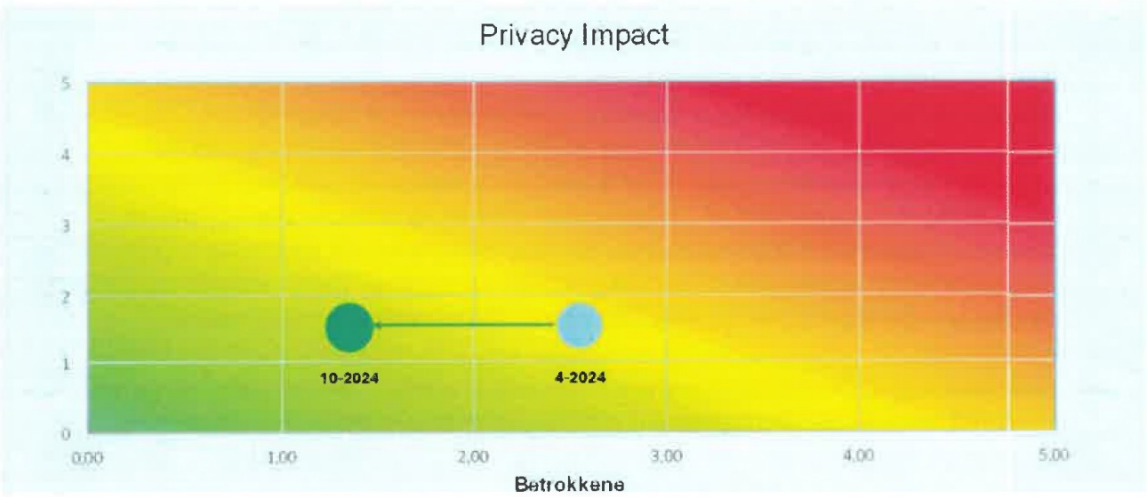
| **Welke maatregelen zijn genomen om de transparantie van de toepassing te borgen?** |
|---|
| Om de transparantie van de toepassing te borgen is Privacy by Design en Default toegepast, worden gebruikers vooraf geïnformeerd, worden toegangslogs bijgehouden en de gegevensverwerking gedocumenteerd. Het naleven van deze maatregelen zorgt ervoor dat gebruikers duidelijk inzicht hebben in wat er met hun gegevens gebeurt, wat essentieel is om vertrouwen in de toepassing te behouden. Wellicht ten overvloede wordt nogmaals vermeld dat in principe geen persoonsgegevens worden verwerkt. |

## 3. Verwerkersovereenkomst

| **Zijn er (verwerkers)overeenkomsten gemaakt met betrokken externe partijen? Zo ja, voeg deze dan toe.** |
|---|
| Niet van toepassing. Alles 'draait' on premise. |

***Algemene opmerking:***

Bij aanvang van de ontwikkeling van de Chatbot MAI is ook een DPIA uitgevoerd. Het resultaat van die DPIA was, dat er sprake was van een redelijk risico (zie de grijze 'dot' in onderstaande afbeelding). De doorontwikkeling van MAI in een on premise omgeving hebben ertoe geleid dat het huidige risico voor betrokkene als verwaarloosbaar kan worden ingeschat (zie de groene 'dot' in onderstaande afbeelding).



## E. Advies Functionaris Gegevensbescherming

Eindoordeel Functionaris voor Gegevensbescherming
Datum: 24 oktober 2024

**Incidentbeheer en maatregelen bij onbedoelde invoer van persoonsgegevens**

- **Advies**: De DPIA vermeldt dat onbedoeld ingevoerde persoonsgegevens zo snel mogelijk worden verwijderd en dat er momenteel wordt gewerkt aan een uitbreiding die automatisch een melding maakt in het geval dat een gebruiker toch persoonsgegevens deelt, welke dan permanent verwijderd zullen worden. Er is echter geen duidelijke procedure voor incidentbeheer voor de chatbot. Wat gebeurt er als persoonsgegevens per ongeluk worden opgeslagen of niet tijdig worden verwijderd? Hoe snel moet een dergelijke situatie worden herkend en gemeld? Dit proces zou explicieter kunnen worden gedefinieerd.
- **Aanbeveling 1**: Ontwikkel en implementeer een procedure voor incidentbeheer die beschrijft hoe snel persoonsgegevens worden gedetecteerd en verwijderd, en welke stappen worden ondernomen om te waarborgen dat dit consistent gebeurt. Zorg ervoor dat deze procedure periodiek wordt getest.
- **Aanbeveling 2**: Geef een concrete tijdsframe waarbinnen de uitbreiding van het systeem zal worden voltooid waarna ingevoerde persoonsgegevens direct automatisch verwijderd zullen worden.
- **Aanbeveling 3**: Laat tot die tijd een gebruiker via een button in de interface zelf melden dat ze (per ongeluk) een persoonsgegeven hebben ingevoerd. Dit werkt veel praktischer dan dat ze achteraf de gemeente moeten bellen of moeten mailen met een PO of FG.

| Startdatum verwerkingen (indien van toepassing) | Wanneer bijwerken register (indien van toepassing) | Datum herziening DPIA (indien van toepassing) |
|---|---|---|
| 14-10-2024 | z.s.m. | 25-10-2024 |

## F. Ondertekening Proceseigenaar

**Naam proceseigenaar:** [redacted]

**Functie:** Domeinmanager Bedrijfsvoering & Dienstverlening

**Datum:** 25.10.2024

**Handtekening:** [redacted]

parell

## Bijlage 1 Risicoclassificatie AI

| Risicoclassificatie AI Chatbot MAI |
|---|
| Dit formulier is bedoeld om een inschatting te maken van het risico van AI. Het is een hulpmiddel en er kunnen geen rechten aan ontleend worden. |
| Versie: Conceptversie 0.1 |
| Auteur: [redacted] |

| 1) Betreft het een AI systeem dat een veiligheidscomponent is van een product of systeem onder de volgende handelingen: |
|---|
| ☐ Beveiliging van de burgerluchtvaart<br>☐ Goedkeuring en markttoezicht op Landbouw- en bosbouwvoertuigen<br>☐ Goedkeuring en markttoezicht op twee, drie en vierwielige voertuigen<br>☐ Maritieme veiligheid en mariene verontreiniging<br>☐ Interoperabiliteit van het Europese spoorwegsysteem<br>☐ Goedkeuring en markttoezicht op motorvoertuigen en aanhangwagens<br>☐ Gemeenschappelijke regels op gebied van de burgerluchtvaart<br>☐ Typegoedkeuring van motorvoertuigen en aanhangwagens |
| Als u één of meer zaken hebt aangevinkt, dan is uitsluitend artikel 84 van de AI Act van toepassing. Uw systeem wordt mogelijk aan bijlage III (hoog risico systemen) toegevoegd. Voor het overige valt uw systeem onder specifieke Europese richtlijnen en/of verordeningen. U hoeft dit formulier dan niet verder in te vullen.<br><br>*Voor meer informatie: Artikel 2, lid 2 AI act.* |

| 2) Is één van onderstaande op u of uw systeem van toepassing? |
|---|
| ☐ Uw systeem wordt louter voor militaire doeleinden ontwikkeld of gebruikt.<br>☐ U bent een overheidsinstantie in een niet EU land of een internationale organisatie én uw AI-systeem wordt gebruikt in het kader van internationale overeenkomsten voor samenwerking met de Unie of een lidstaat op het gebied van rechtshandhaving en justitie. |
| Als u één van deze zaken hebt aangevinkt, dan is de AI Act niet op uw systeem van toepassing. U valt onder specifieke wetgeving.<br>U hoeft dit formulier dan niet verder in te vullen.<br><br>*Voor meer informatie: Artikel 2, lid 3 en 4 AI act.* |

| 3) Is een van de volgende praktijken op uw systeem van toepassing? |
|---|
| ☐ Een AI-systeem dat gedrag van personen wezenlijk verstoort en waarbij personen mogelijk fysieke of psychologische schade oplopen<br>☐ Een AI-systeem dat gebruikmaakt van de kwetsbaarheden van een specifieke groep personen als gevolg van hun leeftijd of fysieke of geestelijke handicap.<br>☐ Een AI-systeem door of namens overheidsinstanties voor de evaluatie of classificatie van de betrouwbaarheid van natuurlijke personen gedurende een bepaalde periode op |

[1] *Met dank aan A. Renkens*

basis van hun sociale gedrag of bekende of voorspelde persoonlijke of persoonlijkheidskenmerken,
☐ Het gebruik van biometrische systemen voor de identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving.

Als u één van deze zaken hebt aangevinkt, dan betreft het mogelijk een verboden praktijk. Raadpleeg Artikel 5 van de AI Act om te bepalen of dit het geval is. Als dat het geval is, stop dan direct met deze praktijk. Als de praktijk bij nadere beschouwing niet verboden is, ga dan verder met dit formulier.

*Voor meer informatie: Artikel 5 AI act.*

**4) Is het AI-systeem bedoeld als veiligheidscomponent van een product of is het zelf een product dat valt onder het volgende?**

☐ Machinerichtlijn
☐ Veiligheid van speelgoed
☐ Pleziervaartuiten en waterscooters
☐ Liften en veiligheidscomponenten daarvan.
☐ Beveiliging van ontploffingsgevaar
☐ Radioapparatuur
☐ Drukapparatuur
☐ Kabelbaaninstallaties
☐ Persoonlijke beschermingsmiddelen
☐ Gasverbrandingstoestellen
☐ Medische hulpmiddelen
☐ Beveiliging burgerluchtvaar
☐ Goedkeuring van en het markttoezicht op twee- of driewielige voertuigen en vierwielers
☐ Goedkeuring van en het markttoezicht op landbouw- en bosbouwvoertuigen
☐ Uitrusting van zeeschepen
☐ Interoperabiliteit van het spoorwegsysteem in de Europese Unie
☐ Goedkeuring en markttoezicht op twee, drie en vierwielige voertuigen
☐ Systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd wat de algemene veiligheid ervan en de bescherming van de inzittenden van voertuigen en kwetsbare weggebruikers betreft
☐ Burgerluchtvaart

**b) Moet er voor het product of het systeem een conformiteitsbeoordeling door een derde partij worden uitgevoerd met het oog op het in de handel brengen of in gebruik stellen van het product of systeem?**

*Voor meer informatie: Bijlage I AI act.*

☐ N.v.t. Ik heb hierboven niets aangekruist.
☐ Ja
☐ Nee

Hebt u hierboven minstens 1 productcategorie aangekruist én hebt u bij vraag b) **Ja** geantwoord? **Uw systeem is een hoog risico systeem**

Zo niet, ga dan verder met invullen.

*Voor meer informatie: Artikel 6, lid 1 AI act.*

**5) Is het AI-systeem bedoeld om-, of werkzaam in de volgende gebieden?**

**Biometrie**

☐ Identificatie op afstand, voor zover het systeem niet als enig doel heeft te bevestigen dat een specifiek natuurlijke persoon de persoon is die deze beweert te zijn.

☐ Categorisering op basis van gevoelige of beschermde eigenschappen of kenmerken, of op basis van wat uit die eigenschappen of kenmerken wordt afgeleid.

☐ Emotieherkenning.

**Kritieke infrastructuur**

☐ Veiligheidscomponent bij het beheer of de exploitatie van kritieke digitale infrastructuur, wegverkeer of bij de levering van water, gas, verwarming en elektriciteit.

**Onderwijs en beroepsopleiding**

☐ Het bepalen van toegang of toelating tot of het toewijzen van natuurlijke personen aan instellingen voor onderwijs.

☐ Beoordelen van het passende onderwijsniveau dat een persoon zal ontvangen of waartoe hij toegang zal hebben..

☐ Monitoren en detecteren van ongeoorloofd gedrag van studenten tijdens toetsen.

**Werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid**

☐ Werven of selecteren van natuurlijke personen, met name voor het plaatsen van gerichte vacatures, het analyseren en filteren van sollicitaties, en het beoordelen van kandidaten.

☐ Het nemen van besluiten die van invloed zijn op de voorwaarden van arbeidsgerelateerde betrekkingen, de bevordering of beëindiging van arbeidsgerelateerde contractuele betrekkingen, voor het toewijzen van taken op basis van individueel gedrag of persoonlijke eigenschappen of kenmerken, of voor het monitoren en evalueren van prestaties en gedrag van personen in dergelijke betrekkingen.

**Essentiële particuliere en publieke diensten en uitkeringen**

☐ Het door of namens overheidsinstanties gebruiken om te beoordelen of natuurlijke personen in aanmerking komen voor essentiële overheidsuitkeringen en -diensten, waaronder gezondheidsdiensten, of om dergelijke uitkeringen en diensten te verlenen, te beperken, in te trekken of terug te vorderen.

☐ Beoordelen van de kredietwaardigheid van natuurlijke personen of voor het vaststellen van hun kredietscore, met uitzondering van AI-systemen die gebruikt worden om financiële fraude op te sporen.

☐ Risicobeoordeling en prijsstelling met betrekking tot natuurlijke personen in het geval van levens- en ziektekostenverzekeringen.

Systemen die bedoeld zijn om noodoproepen van natuurlijke personen te evalueren en te classificeren of om te worden gebruikt voor het inzetten of het bepalen van prioriteiten voor de inzet van hulpdiensten, onder meer van politie, brandweer en ambulance, alsook van systemen voor de triage van patiënten die dringend medische zorg behoeven.

**Rechtshandhaving**

☐ Risico beoordelen dat een natuurlijke persoon het slachtoffer wordt van strafbare feiten.

☐ Gebruik als leugendetector of soortgelijke instrumenten.

☐ Beoordelen van de betrouwbaarheid van bewijsmateriaal tijdens het onderzoek naar of de vervolging van strafbare feiten.

☐ Beoordelen hoe groot het risico is dat een natuurlijke persoon (opnieuw) een strafbaar feit zal plegen , of om persoonlijkheidskenmerken en eigenschappen of eerder crimineel gedrag van natuurlijke personen of groepen te beoordelen.

☐ Natuurlijke personen profileren tijdens het opsporen, onderzoeken of vervolgen van strafbare feiten.

**Migratie-, asiel- en grenstoezicht**

☐ Gebruik als leugendetector of soortgelijke instrumenten.

☐ Risico's beoordelen, waaronder een veiligheidsrisico, een risico op illegale migratie of een gezondheidsrisico, uitgaat van een natuurlijke persoon die voornemens is het grondgebied van een lidstaat te betreden of dat heeft gedaan.

☐ Behandeling van aanvragen voor asiel, visa of verblijfsvergunningen en bij de behandeling van aanverwante klachten in verband met het al dan niet in aanmerking komen van de natuurlijke personen die een aanvraag voor een status indienen, met inbegrip van hieraan gerelateerde beoordelingen van de betrouwbaarheid van bewijsmateriaal.

☐ Het opsporen, herkennen of identificeren van natuurlijke personen, met uitzondering van de verificatie van reisdocumenten.

**Rechtsbedeling en democratische processen**

☐ Ondersteunen bij het onderzoeken en uitleggen van feiten of de wet en bij de toepassing van het recht op een concrete reeks feiten of om te worden gebruikt op soortgelijke wijze in het kader van alternatieve geschillenbeslechting.

☐ Het beïnvloeden van de uitslag van een verkiezing of referendum of van het stemgedrag van natuurlijke personen bij de uitoefening van hun stemrecht bij verkiezingen of referenda. Dit geldt niet voor AI-systemen aan de output waarvan natuurlijke personen niet rechtstreeks worden blootgesteld, zoals instrumenten die worden gebruikt om politieke campagnes te organiseren, te optimaliseren of te structureren vanuit administratief of logistiek oogpunt.

Heb je ergens in vraag 5 een vinkje aangekruist? **Uw systeem is een hoog risico systeem**

Zo niet, ga dan verder met invullen.

*Voor meer informatie: Artikel 6, lid 2 en bijlage III AI act.*

| 6) Is één of meer van de volgende zaken op het systeem van toepassing? |
|---|
| ☐ Uw systeem is bedoeld voor interactie met natuurlijke personen.<br>☐ Uw systeem wordt gebruikt voor emotieherkenning of een biometrische indeling.<br>☐ Uw systeem genereert of bewerkt beeld-, audio- of videomateriaal dat aanzienlijk op bestaande personen, objecten, plaatsen of andere entiteiten of gebeurtenissen lijkt en voor een persoon onterecht als authentiek of waarheidsgetrouw ("deep fake") zou kunnen overkomen. |
| Heb je ergens in vraag 6 een vinkje aangekruist? **Uw systeem is een beperkt risico systeem**<br><br>*Voor meer informatie: Artikel 52 AI act.* |

| 7) Laag risico |
|---|
| Als er niet eerder is uitgekomen dat het systeem de categorisatie verboden, hoog of beperkt risico heeft, dan **is uw systeem een laag risico systeem** in de zin van de AI act. De AI act is verder niet op het systeem van toepassing. Wel is het verstandig om het systeem op te nemen in het interne AI en algoritme register. Daarmee kan de organisatie aantonen dat alle systemen inzichtelijk zijn en beoordeeld zijn op het risico.<br><br>Een laag risico neemt niet weg dat het systeem nog steeds een risico in andere zin kan hebben. Denk daarbij aan privacy, security, inkoop etc. |
| Heb je nergens een vinkje aangekruist? **Uw systeem is een laag risico systeem**<br><br>*Voor meer informatie: Artikel 52 AI act.* |

***Chatbot MAI wordt aangemerkt als een AI-systeem met een laag risico. Dit blijkt ook uit onderstaande tabel, die is ontleend aan de AI-Act. De AI-Act classificeert AI-systemen op basis van hun risiconiveau in verschillende categorieën.***

| Checkpunt | Uitleg | Voorbeelden | Risico-indicatie |
|---|---|---|---|
| Kritieke infrastructuren | AI gebruikt in sectoren zoals energie, transport of waterbeheer. | Slimme netwerken voor elektriciteit in energiebedrijven. | High-risk |
| Productveiligheid | AI-toepassingen geïntegreerd in producten die onder productveiligheidswetgeving vallen, zoals medische apparaten. | AI in chirurgische robots, medische scanners. AI-gebaseerd systeem voor monitoring en onderhoud van slimme verkeersinfrastructuur. | High-risk |
| Rechtshandhaving of strafrecht | AI ingezet door de politie, justitie of voor migratiebeheer. | AI voor criminaliteitsvoorspelling of risicobeoordeling. | High-risk |
| Onderwijs of beroepsopleiding | AI voor het beoordelen van prestaties van leerlingen of studenten. | AI-gebaseerde toetsing en evaluatie in scholen. | High-risk |

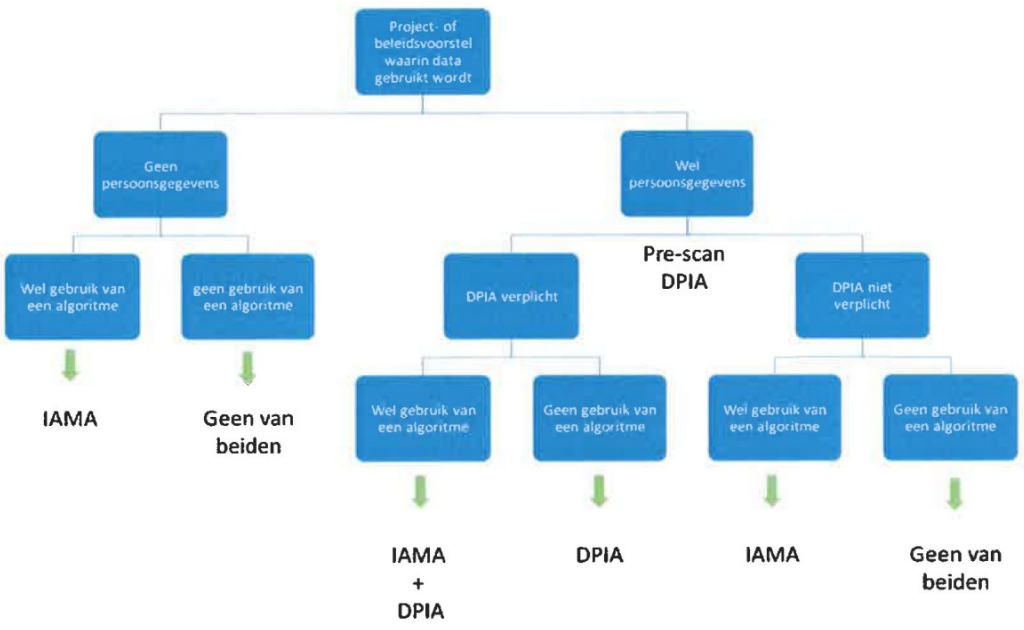
| | | | |
|---|---|---|---|
| Toegang tot essentiële diensten | AI die toegang bepaalt tot diensten zoals werk, leningen, huisvesting of sociale bijstand. | AI voor sollicitatiescreening in een MKB-bedrijf. AI voor het beoordelen van aanvragen voor sociale bijstand of uitkeringen. | High-risk |
| HR-systemen voor werknemersbeslissingen | AI voor het inhuren, promoten of ontslaan van werknemers. | AI voor prestatiebeoordeling van zorgpersoneel. | High-risk |
| Fundamentele rechten beïnvloeden | AI die invloed heeft op grondrechten zoals privacy, vrijheid van meningsuiting. | AI die content modereert op een overheidsplatform. | High-risk |
| Biometrische identificatie op afstand | AI voor biometrische herkenning op afstand, bijvoorbeeld gezichtsherkenning in openbare ruimtes. | Gezichtsherkenning op een luchthaven of in openbare ruimte. | High-risk |
| Onderzoek of interne bedrijfsprocessen | AI voor interne processen of onderzoek zonder directe impact op derden. | Slimmer en sneller zoeken door interne kennisbanken; Detectie van de staat van verkeersborden of bomen, risico gestuurd handhaven; Detectie criminele ondermijning (gericht op bedrijven). | Low-risk |
| Algemene besluitvorming zonder impact | AI voor ondersteuning van beslissingen zonder juridische of substantiële impact. | Automatische categorisering van e-mails en meldingen (MOR); Geautomatiseerde beantwoording raadsvragen. | Low-risk |
| Communicatie, marketing of gepersonaliseerde berichten | Chatbots (gebaseerd op openbare info), AI voor marketing, gepersonaliseerde berichten of aanbevelingssystemen. | ***Chatbots***, AI in aanbevelingssystemen van een webshop of website, vertalen van brieven. | Low-risk |
| Interactief entertainment of recreatie | AI voor puur recreatief gebruik zonder substantiële impact. | AI-gebaseerde games of interactieve assistenten. | No-risk |

# Bijlage 2 Algoritmebeschrijving, zoals opgenomen in het Algoritmeregister

| | |
|---|---|
| **Korte omschrijving** | Mai is een chatbot die 24/7 algemene vragen van burgers beantwoordt op de website van gemeente Montferland. De chatbot vervangt de huidige livechat om wachttijden te verminderen en directe antwoorden te bieden. |
| **Thema** | Organisatie en bedrijfsvoering |
| **Link naar publiekspagina** | |
| **Status** | In ontwikkeling |
| **Doel en impact** | Het doel van Mai is om burgers sneller en 24/7 antwoorden te geven op hun algemene vragen. Dit ontlast de medewerkers op de livechat, zodat zij zich kunnen richten op complexere taken waarvoor menselijke tussenkomst nodig is. De impact is verbeterde dienstverlening en efficiëntere inzet van gemeentelijke middelen. |
| **Afwegingen** | Bij de ontwikkeling van Mai zijn de volgende afwegingen gemaakt:• Kwaliteit van antwoorden in vergelijking met menselijke medewerkers• Correctheid en nauwkeurigheid van de gegeven informatie• Vermogen om binnen het onderwerp te blijven• Naleving van gemeentelijke kernwaarden• Privacy, veiligheid en transparantieEr is een Data Protection Impact Assessment (DPIA) uitgevoerd en een penetratietest door een externe partij om de veiligheid te waarborgen. |
| **Wettelijke basis** | Het leveren van betrouwbare overheidsinformatie over producten en diensten van Gemeente Montferland. |
| **Versie publicatiestandaard** | 1.0 |
| **Link naar bronregistratie** | |
| **Contactgegevens** | [redacted]@montferland.info |
| **Taal** | nld |
| **Link naar broncode** | |
| **Gegevens** | Mai maakt gebruik van de volgende gegevensbronnen:Informatie van de gemeentelijke websiteDe Algemene Plaatselijke Verordening (APV)Aanvullende documenten met gemeentelijke informatie |
| **Technische werking** | Mai is gebaseerd op een RAG-systeem (Retrieval-Augmented Generation) en maakt gebruik van de volgende componenten:Platform: Flowise (open-source, on-premises gehost)Vector Database: Qdrant (open-source, on-premises gehost)Large Language Model (LLM) en Embedding: Azure OpenAI deployments (eigen instantie)Dit systeem stelt Mai in staat om relevante informatie op te halen uit de beschikbare bronnen en deze te combineren met de capaciteiten van het taalmodel om accurate en contextrelevante antwoorden te genereren. |

| | |
|---|---|
| **Menselijke tussenkomst** | In principe functioneert Mai zelfstandig zonder directe menselijke tussenkomst. Echter, de antwoorden van de chatbot worden nauwlettend gemonitord door medewerkers van de gemeente. Feedback van burgers na ieder chatgesprek wordt gebruikt om het systeem continu te verbeteren. |
| **Risicobeheer** | Om risico's te beheersen zijn de volgende maatregelen genomen:Uitvoering van een DPIA (Data Protection Impact Assessment)Externe penetratietest voor veiligheidsvalidatieConstante monitoring van de chatbot-prestatiesMogelijkheid tot direct ingrijpen indien nodigContinue verbetering van kwaliteit en veiligheid op basis van feedback en prestatie-analyses |
| **Leverancier** | Intern ontwikkeld door Gemeente Montferland |
| **Link naar verwerkingsregister** | |
| **Zoektermen** | |
| **Bron-ID** | |
| **Begindatum** | 2024-2 |
| **Einddatum** | |
| **Toelichting op impacttoetsen** | |
| **Publicatiecategorie** | Impactvolle algoritmes |
| **Verwijzingen wettelijke basis** | |
| **Impacttoetsen** | 1: Data Protection Impact Assessment (DPIA) |
| **Verwijzingen gegevensbronnen** | |
| **Algoritme-ID** | 96671359 |

Schema, wel/geen IAMA/DPIA uitvoeren, volgens IAMA- en het model DPIA Rijksdienst, versie 1.0 d.d. 19 januari 2023:



## Bijlage 3 Onderliggende documentatie eerdere DPIA (voorjaar 2024)

Onderstaand zijn links opgenomen naar de onderliggende documenten van de eerder dit jaar uitgevoerde DPIA. De documenten zijn in bijlage bijgevoegd.

DPIA - AI - Gemeente Monfortlar

DPIA - AI - Gemeente Monfortlar

DPIA - AI - Gemeente Monfortlar

DPIA - AI - Gemeente Monfortlar