

Managementsamenvatting – Beveiligingsmaatregelen Joni RAG

Joni gebruikt Retrieval-Augmented Generation (RAG) om persoonsgegevens tijdelijk op te halen uit JOIN voor betere antwoorden, maar slaat deze niet op en leert er niet van.

De belangrijkste beveiligingsmaatregelen zijn:

- OAuth-authenticatie: Joni gebruikt exact dezelfde rechten als de ingelogde JOIN-gebruiker.
- TLS-versleutelde communicatie tussen Joni, JOIN en het AI-model.
- Logging optioneel en met sanitizer: alle persoonsgegevens worden verwijderd vóór opslag; gebruikers worden alleen met een interne item key geïdentificeerd.
- Geen extra opslag van persoonsgegevens buiten JOIN; AI-context verdwijnt direct na beantwoording.
- Toegang tot auditlogs is strikt beperkt tot bevoegde JOIN-beheerders.

Conclusie: de RAG-functionaliteit voegt geen nieuwe privacyrisico's toe en blijft volledig binnen de AVG en de Europese AI-wetgeving.

Data Protection Impact Assessment (DPIA) – Joni RAG-functionaliteit

1. Doel en rechtmatigheid

De AI-chatbot Joni ondersteunt gebruikers bij het vinden en begrijpen van informatie binnen het JOIN-systeem. Met de nieuwe Retrieval-Augmented Generation (RAG)-functionaliteit kan Joni ook persoonsgegevens gebruiken, uitsluitend voor het geven van contextuele antwoorden aan de gebruiker die daar al toegang toe heeft.

Deze verwerking is noodzakelijk om de efficiëntie en bruikbaarheid van JOIN te verbeteren en blijft binnen de bestaande doelbinding van het systeem. Er worden geen nieuwe persoonsgegevens verzameld of permanent verwerkt buiten JOIN. Joni fungeert als een slimme zoek- en antwoordlaag.

2. Beschrijving van de verwerking

1. De gebruiker stelt een vraag aan Joni.
2. Joni voert een realtime zoekopdracht uit via de beveiligde JOIN REST API, met de rechten van de ingelogde gebruiker.
3. Alleen records waartoe de gebruiker toegang heeft, worden opgehaald (inclusief eventuele persoonsgegevens).
4. De relevante tekstfragmenten worden tijdelijk als context toegevoegd aan de prompt van het AI-model.
5. Het AI-model genereert een antwoord, waarna de context niet wordt opgeslagen of hergebruikt.

Belangrijke randvoorwaarden:

- Geen persoonsgegevens in embeddings → Alleen anonieme zaaktype-namen zijn vooraf ge-embed.
- Geen training of fine-tuning van het AI-model met persoonsgegevens.
- Alle persoonsgegevens blijven uitsluitend in JOIN en vallen onder bestaande toegangsrechten.

3. Betrokkenen en gegevens

Categorieën betrokkenen:

- Burgers, medewerkers of andere natuurlijke personen waarvan gegevens in JOIN zijn opgeslagen.

Categorieën persoonsgegevens:

- Afhankelijk van de vraag: namen, adressen, contactgegevens, zaakgegevens, mogelijk bijzondere persoonsgegevens zoals beschreven in de bestaande verwerkersovereenkomsten.

4. Noodzaak en proportionaliteit

De verwerking is noodzakelijk om gebruikers van JOIN efficiënter te ondersteunen in hun werk. Er worden geen nieuwe gegevens verzameld; Joni gebruikt alleen informatie die de gebruiker toch al kan inzien via de normale JOIN-interface. De verwerking is beperkt: persoonsgegevens worden niet opgeslagen maar slechts tijdelijk gebruikt voor het specifieke antwoord.

5. Risicoanalyse

Risico	Toelichting	Kans	Impact
Ongeautoriseerde toegang via Joni	AI toont gegevens aan iemand zonder rechten	Laag	Hoog
Onbedoelde onthulling in AI-antwoorden	AI kan irrelevante persoonsgegevens meenemen in een antwoord	Middel	Middel
Opslag of hergebruik van gevoelige data	AI zou data onthouden en later hergebruiken	Laag	Hoog
Profiling of secundair gebruik	Data uit AI-conversaties wordt elders gebruikt	Laag	Hoog

6. Mitigerende maatregelen

- Toegangscontrole: Joni haalt gegevens alleen op via de JOIN API, die gebruikersrechten afdwingt.
- Geen persistente opslag: persoonsgegevens worden niet in Joni of in embeddings opgeslagen en verdwijnen direct na beantwoording.
- AI-model is niet getraind op persoonsgegevens: er vindt geen fine-tuning plaats met gevoelige data.
- Beveiligde communicatie: API-verkeer is TLS-versleuteld, en logs bevatten geen inhoudelijke persoonsgegevens.
- Functionele beperkingen: Joni toont alleen korte contextfragmenten en geen volledige dossiers tenzij expliciet gevraagd.
- Bewustwording en beleid: gebruikers worden geïnformeerd over wat Joni wel/niet doet en dat AI-antwoorden nooit meer rechten geven dan de JOIN-interface.
- Joni en de bijbehorende componenten zijn door een externe partij aan een penetratietest onderworpen.

7. Technische en organisatorische beveiligingsmaatregelen

Authenticatie en autorisatie

Joni logt altijd in als dezelfde gebruiker die geauthentiseerd is in JOIN. Hiervoor wordt OAuth gebruikt, waardoor Joni nooit bredere toegang heeft dan de gebruiker zelf. Dit voorkomt ongeautoriseerde toegang tot persoonsgegevens.

Beveiliging van communicatie

Alle communicatie tussen Joni, de JOIN REST API en de AI-componenten is TLS-versleuteld. Er worden geen gevoelige gegevens in URL's of headers geplaatst die kunnen uitlekken via logging of monitoring.

Logging en audittrail

Chatvragen en AI-antwoorden kunnen optioneel worden gelogd voor auditdoeleinden. Hierbij wordt een sanitizer toegepast die alle persoonsgegevens verwijdert voordat de tekst wordt opgeslagen. Om de gebruiker in het log te identificeren wordt geen naam gebruikt, maar een item key, die alleen door een JOIN-beheerder kan worden herleid tot een specifieke gebruiker.

Beperking van opslag

Persoonsgegevens die via RAG tijdelijk aan het AI-model worden aangeboden, worden niet opgeslagen of hergebruikt. Na beantwoording verdwijnen deze gegevens direct uit het geheugen van het AI-model.

Beheer en toegang

Alle beheeractiviteiten rondom Joni zijn beperkt tot bevoegde systeembeheerders. Logs met geanonimiseerde gegevens zijn alleen in te zien door een beperkt aantal geautoriseerde medewerkers.

8. Rest-risico en conclusie

Met bovenstaande opzet zijn de risico's voor privacy laag tot aanvaardbaar, omdat:

- Alleen geautoriseerde gebruikers toegang krijgen tot dezelfde gegevens als in JOIN.
- De verwerking tijdelijk en doelgebonden is.
- Er geen nieuwe opslag of trainingsdataset ontstaat.

Deze DPIA toont aan dat het gebruik van RAG in Joni voldoet aan de AVG en de Europese AI-wetgeving. Daarnaast zijn extra technische en organisatorische maatregelen geïmplementeerd, zoals OAuth-gebaseerde authenticatie, versleutelde communicatie, geanonimiseerde logging en strikte toegangscontrole.