DPIA (Data Processing Impact Assessment) voor KISS (Klant Interactie Service Systeem)

Datum: 21 augustus 2023

Ingevuld door: Ramon Fasel

Projectgegevens

Gewenste functionaliteit	Applicatie om een klantcontactcentrum te ondersteunen bij het afhandelen en registreren van contactmomenten en -verzoeken.
Aanleiding	Het oude systeem was verouderd.
Doelstelling	Gegevens van medewerkers kunnen doorzoeken om contactverzoeken te kunnen versturen
Scope persoonsgegevens en vertrouwelijkheid	Medewerkersgegevens

Lijst met verwerkingen

- Indexeren van gegevens van medewerker in Elastic
- Opvragen gegevens uit de Basisregistratie Personen (BRP), OpenZaak, OpenKlant, Objects
- Opslaan gegevens in OpenKlant, Objects via een API
- Caching van gegevens

Indexeren van gegevens van medewerker in Elastic

Verwerking persoonsgegevens	
Doel van de verwerking	Informatie van de medewerker indexeren om deze doorzoekbaar maken. Indexeren gebeurt door gegevens periodiek te posten naar Elastic (lokaal gehost)
Persoonsgegevens die worden verwerkt	• Volledige naam van medewerker • E-mailadres en telefoonnummer werk • Werktijden, functie, afdeling, specialisaties, naam vervanger

Risico's van verwerking	Extra mogelijke tegenmaatregelen	Tegenmaatregelen genomen
Elastic index wordt ontsloten via een andere website/applicatie zodat gegevens opgevraagd kunnen worden	[beschrijf tegenmaatregelen inclusief gepland of niet gepland]	[beschrijf genomen tegenmaatregelen]
Gegevens van de medewerker worden opgevraagd via een API, zie risico bij sectie Opvragen gegevens Objects hieronder.	Zie risico bij sectie Opvragen gegevens Objects hieronder.	Zie risico bij sectie Opvragen gegevens Objects hieronder.

Opvragen gegevens uit de Basisregistratie Personen (BRP), OpenZaak, OpenKlant, Objects

Verwerking persoonsgegevens	
Doel van de verwerking	• BRP: ophalen persoonsgegevens om de identiteit van de persoon die contact heeft opgenomen te verifiëren en het contactmoment aan die persoon te koppelen. • Overige: ophalen gegevens uit bron om te tonen aan de KCM (klantcontactmedewerker)

Persoonsgegevens die worden verwerkt	• BRP: volledige naam, bsn, geboortedatum, geboorteplaats, geboorteland, adres
	• OpenZaak: volledige naam, naam van behandelaar, toelichting*
	• OpenKlant: telefoonnummer, e-mailadres, notitie*, naam medewerker
	• Objects:
	  ○ Interne taak: 2x toelichting*, volledige naam, e-mailadres, telefoonnummer, werktelefoonnummer, naam medewerker
	  ○ Medewerker: volledige naam, e-mailadres en telefoonnummer werk, werktijden, functie, afdeling, specialisaties

* open tekstvelden waar gevoelige informatie in kan staan

Het opvragen van gegevens via een API brengt standaard verschillende risico's met zich mee.

Risico's van verwerking	**Extra mogelijke tegenmaatregelen**	**Tegenmaatregelen genomen**
Ongeautoriseerde toegang: Als er onvoldoende beveiligingsmaatregelen zijn geïmplementeerd, kunnen ongeautoriseerde personen of systemen toegang krijgen tot de persoonsgegevens die via de API worden opgevraagd.	• Beveiligingsaudits: Voer regelmatig beveiligingsaudits uit om zwakke punten in het systeem te identificeren en aan te pakken. • Toezicht en monitoring: Bewaak de opvragingen en activiteiten via de API om ongebruikelijke patronen of verdachte activiteiten te	• Sterke authenticatie en autorisatie: Zorg ervoor dat alleen geautoriseerde gebruikers toegang hebben tot de opgevraagde gegevens. • Versleutelde communicatie: Gebruik versleuteling om de gegevens tijdens verzending te beschermen.

	detecteren. (Dit wordt logging voor verwerking) • Gegevensminimalisatie: Vraag alleen de minimale hoeveelheid gegevens op die nodig zijn voor het beoogde doel. Op dit moment worden er mogelijk teveel zaakgegevens opgevraagd.	• Juridische naleving: Zorg ervoor dat de opvragende partij zich houdt aan relevante privacyregelgeving en ethische normen bij het verwerken van persoonsgegevens.
Datalekken: Als de API kwetsbaarheden bevat of als er zwakke beveiligingsprotocollen zijn, kunnen kwaadwillende personen toegang krijgen tot de opgevraagde persoonsgegevens, wat kan leiden tot datalekken en inbreuken op de privacy.	Zie eerste punt	Zie eerste punt
Overdracht van gegevens via onveilige kanalen: Als de communicatie tussen de opvragende partij en de API niet goed is beveiligd, kunnen gegevens tijdens de overdracht worden onderschept door aanvallers.	Zie eerste punt	Zie eerste punt
Verkeerde opslag van gegevens: De opvragende partij moet ervoor zorgen dat	Zie eerste punt	Zie eerste punt

de opgevraagde persoonsgegevens op een veilige manier worden opgeslagen en dat er passende beveiligingsmaatregelen worden genomen om ongeautoriseerde toegang te voorkomen.		
Onvoldoende gegevensbescherming: Als de API-provider geen passende beveiligingsmaatregelen heeft geïmplementeerd, kunnen de persoonsgegevens die via de API worden opgevraagd, blootgesteld worden aan externe bedreigingen.	Zie eerste punt	Zie eerste punt
Verkeerde gegevensverwerking: Als de opvragende partij de persoonsgegevens niet op een wettige en ethische manier verwerkt, kan dit leiden tot schendingen van de privacywetgeving en reputatieschade.	Zie eerste punt	Zie eerste punt
Naleving van privacyregelgeving: Als de opvragende partij persoonsgegevens opvraagt zonder rekening te houden met de toepasselijke privacyregelgeving, kunnen	Zie eerste punt	Zie eerste punt

juridische consequenties volgen, zoals boetes en juridische procedures.		

Opslaan gegevens in OpenKlant, Objects via een API

Verwerking persoonsgegevens	
Doel van de verwerking	Vastleggen van klanten, contactmomenten en -verzoeken

Persoonsgegevens die worden verwerkt	• OpenKlant: telefoonnummer, e-mailadres, notitie*, naam medewerker
	• Objects:
	  ○ Interne taak: 2x toelichting*, volledige naam, e-mailadres, telefoonnummer, werktelefoonnummer, naam medewerker
	  ○ Medewerker: volledige naam, e-mailadres en telefoonnummer werk, werktijden, functie, afdeling, specialisaties

Het sturen van gegevens naar een API brengt standaard verschillende risico's met zich mee.

Risico's van verwerking	**Extra mogelijke tegenmaatregelen**	**Tegenmaatregelen genomen**
Ongeautoriseerde toegang: Als persoonsgegevens via een API worden verzonden, bestaat het risico dat ongeautoriseerde personen toegang krijgen tot deze gegevens als de API onvoldoende beveiligd is. Onvoldoende authenticatie en autorisatie kunnen leiden tot	• Regelmatige beveiligingsscans en tests: Uitvoeren van beveiligingstests en regelmatige audits om kwetsbaarheden op te sporen en te verhelpen. Dit valt straks onder beheer.	• Sterke authenticatie en autorisatie: Gebruik van sterke identificatiemethoden om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot de gegevens.

datalekken en inbreuken op de privacy.	• Transparantie: Duidelijke informatie verstrekken aan gebruikers over gegevensverzameling, -verwerking en -opslag via de API. Dit valt onder het werkproces. • Toezicht en monitoring: Actieve monitoring van de API om ongebruikelijke activiteiten te detecteren en te voorkomen.	• Versleutelde communicatie: Gebruik van versleuteling om ervoor te zorgen dat de gegevens tijdens verzending veilig zijn. • Gegevensminimalisatie: Alleen relevante gegevens moeten worden verzonden en verwerkt.
Datalekken: Als er zwakke beveiligingsmaatregelen zijn getroffen of als de API kwetsbaarheden heeft, kunnen kwaadwillende personen of hackers mogelijk toegang krijgen tot persoonsgegevens. Dit kan leiden tot datalekken en de diefstal van gevoelige informatie.	Zie eerste punt	Zie eerste punt
Onbedoelde gegevensverspreiding: Als de API niet goed is geconfigureerd, kan het mogelijk persoonsgegevens delen met onbedoelde derde partijen. Dit kan voortkomen	Zie eerste punt	Zie eerste punt

uit fouten in de code of misconfiguraties van de API.		
Gegevensintegriteit: Gegevens die via een API worden verzonden, kunnen tijdens het verzendproces worden gemanipuleerd of gewijzigd, wat de integriteit van de gegevens in gevaar kan brengen.	Zie eerste punt	Zie eerste punt
Opslag van gegevens: Als de ontvangende partij van de API de verzonden persoonsgegevens niet adequaat beveiligt, kunnen de gegevens kwetsbaar zijn voor misbruik of diefstal nadat ze zijn ontvangen.	Zie eerste punt	Zie eerste punt
Onvoldoende transparantie: Het is belangrijk om transparant te zijn over welke gegevens worden verzameld, hoe ze worden verwerkt en met wie ze worden gedeeld via de API. Het ontbreken van duidelijke informatie kan leiden tot problemen met naleving van privacyregelgeving.	Zie eerste punt	Zie eerste punt
Internationale gegevensoverdracht: Als persoonsgegevens worden verzonden naar een API die zich buiten de jurisdictie van	Zie eerste punt	Zie eerste punt

de gegevensbron bevindt, kunnen er uitdagingen zijn met betrekking tot de naleving van internationale privacywetten en regelgeving.		

Caching van gegevens

Verwerking persoonsgegevens	
Doel van de verwerking	Het tijdelijk opslaan van gegevens voor herhaald gebruik, om de prestaties van het systeem te verbeteren.
Persoonsgegevens die worden verwerkt	• [nog in te vullen als we gaan cachen]

Het cachen van gegevens brengt standaard verschillende risico's met zich mee.

Risico's van verwerking	**Extra mogelijke tegenmaatregelen**	**Tegenmaatregelen genomen**
Ongeoorloofde toegang tot cache: Als de cache niet goed is beveiligd, kan ongeautoriseerde toegang tot de opgeslagen persoonsgegevens plaatsvinden. Dit kan gebeuren als kwaadwillende personen of systemen toegang krijgen tot de cachegegevens.	• Privacy Impact Assessment (PIA): Voer een PIA uit om de potentiële privacy-impact van het cachen van persoonsgegevens te evalueren en passende maatregelen te nemen. • Gegevensminimalisatie: Cache alleen de strikt noodzakelijke gegevens en minimaliseer het	Nog geen, want geen caching.

	opslaan van gevoelige persoonsgegevens. • Beveiliging: Implementeer sterke beveiligingsmaatregelen om ongeautoriseerde toegang tot de cache te voorkomen, inclusief autorisatie en authenticatie. • Cachebeheer: Stel beleid en procedures op voor het beheer van de cache, inclusief het verwijderen van verouderde of niet langer relevante gegevens. • Tijdsbeperkingen: Implementeer tijdsbeperkingen voor hoe lang gegevens in de cache worden bewaard, om te voorkomen dat verouderde informatie wordt weergegeven. • Versleuteling: Versleutel gegevens die in de cache worden opgeslagen, zodat zelfs als de	

	cache wordt gecompromitteerd, de gegevens moeilijker te interpreteren zijn. • Monitoring en audits: Houd toezicht op de cache-activiteiten en voer regelmatige beveiligingsaudits uit om zwakke punten op te sporen en te verhelpen.	
Verouderde gegevens: Omdat gecachte gegevens oudere versies van de werkelijke gegevens kunnen weerspiegelen, bestaat het risico dat gebruikers verouderde of onjuiste informatie te zien krijgen, wat de juistheid en integriteit van de gegevens in gevaar kan brengen.	Zie eerste punt	Zie eerste punt
Inconsistentie: Als dezelfde gegevens in verschillende delen van het systeem worden gecached, kan inconsistentie ontstaan wanneer gegevens worden bijgewerkt. Dit kan leiden tot verwarrende of tegenstrijdige informatie voor gebruikers.	Zie eerste punt	Zie eerste punt
Privacyrisico's: Als persoonsgegevens worden	Zie eerste punt	Zie eerste punt

opgeslagen in de cache zonder voldoende anonimisering of pseudonimisering, kunnen deze gegevens toegankelijk zijn voor iedereen die toegang heeft tot de cache, waardoor de privacy van individuen in gevaar kan komen.		
Gegevenslekken: Als de cache per ongeluk of door kwaadwillende acties wordt blootgesteld, kunnen persoonsgegevens gemakkelijk worden gestolen of gelekt, wat kan leiden tot ernstige inbreuken op de gegevensbescherming.	Zie eerste punt	Zie eerste punt
Nalevingsproblemen: Als de opslag van persoonsgegevens in de cache niet in overeenstemming is met de geldende privacyregelgeving, kan dit leiden tot juridische en regelgevende problemen, zoals schendingen van de Algemene Verordening Gegevensbescherming (AVG) in Europa.	Zie eerste punt	Zie eerste punt