Datum	4 april 2025
Behandeld door	Ambtelijk secretaris
E-mail	cpa@amsterdam.nl

Onderwerp Het programma Prima: Voicebot en Chatbot

Advies van de Commissie Persoonsgegevens Amsterdam (CPA) over het programma Prima: Chatbot en Voicebot. Het agendapunt is behandeld op de openbare vergadering van 21 november 2024.

Geachte heer 5.1, 2, e

Tijdens de vergadering van de CPA van 21 november 2024 was u aanwezig bij het agendapunt "Het programma Prima: Voicebot en Chatbot".

Bijgaand treft u aan het advies van de CPA.

A. Samenvatting advies

De commissie geeft u de volgende **adviezen** ter overweging mee:

- verricht nader onderzoek naar de herkomst van de trainingsdata en de juridische status met betrekking tot auteursrechten en persoonsgegevens;
- leg expliciet vast welke partij welke verantwoordelijkheden draagt bij het gebruik van de spraakherkenningssoftware en maak afspraken over het naleven van de AVG bij het verzamelen van trainingsdata;
- bied burgers het alternatief om met een medewerker te kunnen communiceren door hier helder en transparant over te communiceren en deze keuze bij aanvang van het gesprek expliciet aan te bieden;
- gebruik AI/robotisering zorgvuldig en verantwoord, wees bewust van de risico's en neem actief maatregelen om deze te beperken.

De Commissie:

- wenst te vernemen op welke wijze de gemeente Amsterdam gevolg heeft gegeven aan haar adviezen.

B. Aanleiding en omschrijving

Er heeft een eerder bezoek plaatsgevonden bij de CPA (*d.d. 11-4-2024*). Naar aanleiding van dit bezoek is gevraagd of het onderdeel voicebot van de Omnichannel nader kan worden toegelicht bij de CPA. De voicebot is reeds sinds januari 2024 in gebruik en per februari 2025 zal ook een chatbot en het kanaal live chat worden toegevoegd aan de Omnichannel Dienstverlening. Beide functionaliteiten lijken op elkaar maar zijn toch verschillend, daarom zijn ook 2 aparte DPIA's opgesteld. De voicebot hoort bij het proces Omnichannel van Dienstverlening. Dit proces gaat over de dienstverlening aan burgers, bezoekers en ondernemers die direct contact opnemen met de gemeente via verschillende communicatiekanalen. Het gaat hier om een specifiek onderdeel van het communicatiekanaal telefonie, namelijk de voicebot. De chatbot hoort tevens bij het

proces Omnichannel van Dienstverlening. Echter, heeft deze betrekking op een nieuw communicatiekanaal voor burgers, bezoekers en ondernemers: de chat.

Doel van de verwerking van persoonsgegevens

De voicebot- en chatfunctie zijn onderdeel van het gehele proces van leveren van dienstverlening aan burgers, bezoekers en ondernemers (omnichannel). Het overkoepelende doel hiervan is dat goede dienstverlening volgens de gemeente **persoonlijk**, eenvoudig en toegankelijk moet zijn.

Hier kunnen 2 subdoelen onder worden geschaard.

1. Persoonlijke dienstverlening: de gemeente wenst agents te informeren of bellers/mailers reeds eerder contact hebben opgenomen, zodat zij hier rekening mee kunnen houden en indien nodig meer empathie kunnen tonen. Dit draagt bij aan het leveren van een meer persoonlijke, eenvoudige en toegankelijke dienstverlening.
2. Anonieme/geaggregeerde (trend)analyses maken: loggingsgegevens worden gebruikt om trendanalyses en operationele rapportages op te stellen ten behoeve van sturing en verbetering van de dienstverlening.

Verwerkingsgrondslag

De verwerking van persoonsgegevens vindt plaats op grond van artikel 6 lid 1 sub e AVG. Taken van algemeen belang houden verband met taken die worden uitgevoerd door instanties die belast zijn met een publieke taak. Hier kan de dienstverlening van de gemeente onder worden geschaard.

De verwerking van persoonsgegevens vindt tevens plaats op grond van artikel 6 lid 1 sub c AVG. Personen die contact opnemen met de gemeente doen dit om informatie te vragen over producten of diensten die verband houden met de wettelijke taak van de gemeente dan wel om een product of dienst van de gemeente aan te vragen. Denk hierbij aan onderwerpen op het gebied van gemeentebelasting, afval, burgerzaken en parkeren. Dit sluit aan bij de wettelijke verplichting van de gemeente.

Verzoek aan de CPA

De CPA wordt verzocht kennis te nemen van de DPIA omnichannel voicebot en de DPIA omnichannel chatbot. De gemeente Amsterdam stelt daarbij de volgende vragen:

- Aangezien chat een nieuw kanaal is voor de gemeente willen wij graag weten of we nog potentiële risico's missen in onderdeel 11 (Risico's en maatregelen) van de aangeleverde DPIA (2024 DPIA Omnichannel chat).
- Hoe kijkt de CPA aan tegen het (en hoe) omgaan met AI/robotisering oplossingen zoals voicebot en chatbot bij overheidsorganisaties in zijn algemeenheid.

C. Advies

De CPA dankt de bij dit adviesverzoek betrokken medewerkers van de gemeente voor hun toelichting en de aangeleverde stukken.

Gespreksopnamen

Er wordt geen gebruik gemaakt van stemherkenning, maar wel van spraakherkenning. De leverancier van de spraakherkenningssoftware heeft een basismodule ontwikkeld op basis van miljoenen stemmen uit de hele wereld, maar het is onbekend waar deze stemmen precies vandaan komen en in hoeverre dit verenigbaar is met auteursrechten en privacywetgeving.

Er bestaat dus onduidelijkheid over de herkomst van de spraakdata die gebruikt is om de software te trainen. Ook is niet duidelijk of hiervoor verantwoordelijkheid bij de gemeente ligt. De CPA adviseert om nader onderzoek te doen naar de herkomst van de spraakdata en de juridische status met betrekking tot auteursrechten en het recht op bescherming van persoonsgegevens.

De CPA ziet het vanuit het perspectief van gegevensbescherming als positief dat is vastgelegd dat de door de gemeente verzamelde gegevens niet gebruikt mogen worden voor verdere training van het model. Desondanks beveelt de CPA aan om expliciet vast te leggen welke partij welke verantwoordelijkheden draagt bij het gebruik van de software en afspraken te maken over het naleven van de AVG bij het verzamelen van spraakdata.

Transparantie over gebruik chatbot

Transparantie over het gebruik van geautomatiseerde systemen is essentieel om het vertrouwen van burgers te behouden. Daarnaast is de gemeente op grond van artikel 50 lid 1 van de AI-verordening verplicht om bij de inzet van chatbots duidelijk te maken dat gebruikers met AI communiceren. Burgers moeten er bewust van worden gemaakt dat ze communiceren met een machine, zodat ze een weloverwogen beslissing kunnen nemen.

Vanuit ethisch oogpunt geeft de CPA voorkeur aan dat de burger waar mogelijk de optie wordt geboden te kiezen uit contact met een chatbot of contact met een medewerker. Om dit te waarborgen, worden door de gemeente verschillende teksten ingebouwd die aangeven dat deze keuze bestaat. De gemeente onderzoekt continu welke formuleringen het meest effectief zijn, onder andere door maandelijkse rapportages van klanttevredenheidsonderzoeken uit een burgerpanel te analyseren. Ook wordt gewerkt aan een ethische bijsluiter.

De CPA merkt op dat het belangrijk is burgers een alternatief te bieden voor interactie met een AI-systeem. De burger moet de mogelijkheid hebben om direct met een medewerker te spreken. Hiervoor moet duidelijke en ondubbelzinnige communicatie worden gebruikt. Dit betekent dat de keuze bij aanvang van het gesprek expliciet moet worden aangeboden en eenvoudig beschikbaar moet zijn. Dit kan bij een telefoongesprek

door in een keuzemenu hierover te informeren en een optie te bieden om direct met een medewerker te spreken. Via de chatfunctie kan dit worden geborgd door aan het begin van de chat, voor aanvang van het gesprek, de mogelijkheid te bieden over te stappen naar een chat met een medewerker.
Tot slot is de CPA geïnteresseerd in de verdere ontwikkeling van de ethische bijsluiter en wil zij graag betrokken worden bij de volgende sessie.

Het gebruik van AI/robotisering door overheidsorganisaties

De gemeente is benieuwd naar de algemene visie van de CPA op de inzet van AI/robotisering door gemeenten. Volgens de CPA brengt de inzet van AI door overheidsorganisaties zowel kansen als risico's met zich mee.

Efficiëntieverbetering is een legitiem doel, maar mag niet ten koste gaan van de toegankelijkheid van de overheid voor burgers. De keuzevrijheid van burgers moet gewaarborgd blijven. Daarnaast spelen - mogelijke risico's voor de bescherming van persoonsgegevens een belangrijke rol, met name bij de training van AI-modellen met data die persoonsgegevens bevat. Wanneer een externe partij wordt ingeschakeld, wordt het toezicht op het gebruik van persoonsgegevens lastiger en is de gemeente meer afhankelijk van een derde, terwijl de gemeente als opdrachtgever wel verwerkingsverantwoordelijke is (en blijft). Van belang is dat de gemeente altijd verantwoording moet kunnen afleggen over de herkomst en verwerking van persoonsgegevens, ook wanneer een externe partij is ingeschakeld. Met deze derde dienen afspraken te worden gemaakt om de bescherming van de persoonsgegevens conform de vereisten van de AVG.

De CPA ziet op zichzelf geen bezwaar tegen het gebruik van AI door overheidsorganisaties, mits dit zorgvuldig en verantwoord gebeurt. De gemeente dient zich bewust te zijn van de risico's en actief maatregelen te nemen om deze te beperken. Dit betekent dat:

- burgers altijd een reëel alternatief moeten hebben voor op AI gebaseerde interacties;
- volledige transparantie moet bestaan over de werking en herkomst van de gebruikte modellen en datasets;
- de gemeente controle moet houden over de verwerking van persoonsgegevens en risico's op bias moet minimaliseren;
- de gemeente als opdrachtgever voor de training van modellen verwerkingsverantwoordelijke is, ook wanneer externe partijen betrokken zijn.

Tot slot

Verder verwijst de CPA u naar bijgevoegde notulen van de vergadering over het betreffende agendapunt.

Hoogachtend,

Mevrouw H. Janssen
Voorzitter Commissie Persoonsgegevens Amsterdam

Uittreksel van het verslag van het 6e agendapunt van de vergadering op donderdag 21 november 2024

6. Het programma PRIMA: Chatbot en Voicebot

Dit programma is eerder in de CPA geweest vanwege de aan sluiting op de BRP. De commissie heeft toen gevraagd om deze nadere toelichting op het onderdeel voicebot van het omnichannel programma ter verbetering van de informatieverstrekking aan de burgers. In januari is de voicebot toegevoegd en het is de bedoeling de chatbot in komende februari in te voeren. Daarna gaat men werken aan de verbetering van de formulieren en de loketten. Het achterliggende idee is dat de burger niet bij elk nieuw contactmoment met een gemeentelijke dienst – per telefoon of mail, bij een loket of via een formulier – telkens weer zijn hele verhaal en gegevens opnieuw hoeft te vertellen. Het programma is als het ware een schakel tussen de vraag van de burger en de dertig applicaties waarin de verschillende diensten hun zaken opslaan, zonder dat de burger in die applicaties zelf kan gaan rondneuzen. De vraag en de gegevens worden één keer opgenomen, als de burger daar toestemming voor geeft, en daarna wordt die vraag beantwoord door de chatbot, als het gaat om een bekende vraag waarop vooraf een antwoord geformuleerd is. Als de chatbot het antwoord niet in het databestand heeft, volgt een doorverwijzing of doorverbinding naar de juiste persoon. Het databestand is gevoed en met vragen en antwoorden en getraind door medewerkers die intensief hebben gebeld om te testen. Bij validatie is gebleken dat 90% van de vragen goed afgehandeld werden.

De CPA vraagt wat er gebeurt met de opname van de burger en zijn verstrekte gegevens.

Er wordt niet gewerkt met stemherkenning. De opname wordt 28 dagen opgeslagen en kan worden gebruikt voor analyses van de vragen die gesteld worden of bij de behandeling van een bezwaar van de betreffende beller. Een en ander staat beschreven in de privacyverklaring.
Het programma doet wel aan spraakherkenning in die zin dat het getraind is de inhoud van een vraag te herkennen ongeacht de stem of tongval van een beller. Voor die spraakherkenning heeft de leverancier van het programma een basismodule ontwikkeld aan de hand van miljoenen stemmen uit de hele wereld. Wellicht dat Deloitte, dat voor de gemeente het programma uitvoert, weet waar die stemmen precies vandaan komen en hoe het dan staat met auteursrechten en persoonsgegevens. De aanwezigen waren daar niet bij en men weet ook niet of er sprake is van gebruikersverantwoordelijkheid. Wel is vastgelegd dat de gegevens die de gemeente met dit programma verzamelt, niet gebruikt mogen worden voor training van het model.

De CPA vraagt hoe een burger weet dat er een functionaliteit is om met een mens in plaats van een robot te spreken. Wettelijk gezien moeten burgers altijd dat alternatief hebben. De eerste vraag in een telefoongesprek zou bijvoorbeeld kunnen zijn dat men kan kiezen of men verbonden wil worden met een medewerker of met een chat. Er worden verschillende teksten ingebouwd om dat te laten weten. Elke maand komen er rapportages van het klanttevredenheidsonderzoek van een burgerpanel die geanalyseerd worden. Zo komt men te weten welke teksten het best gehanteerd kunnen worden. Ook wordt er gewerkt aan een ethische bijsluiter. In het begin adviseerden leverancier Poly AI en uitvoerder Deloitte bellers vooral er niet op te attenderen dat men in contact zou worden gebracht met een robot, omdat dit tot veel afhakers zou leiden. Daarop heeft de gemeente een proef gedaan met twee panels en daarna besloten toch melding te maken van de inzet van een robot. Dit omdat men zo transparant en eerlijk mogelijk wil zijn. Ook in UX praat de gemeente met burgers over dit soort onderwerpen om te perfectioneren en gebruiksvriendelijker te maken wat de professionals in de business zoal voor ze

De CPA wil graag uitgenodigd worden voor een volgende sessie over de ethische bijsluiter bij die programma. Dat zal gebeuren, wordt toegezegd.
De CPA is benieuwd of de geluidsopname en het transcript beschouwd worden als persoonsgegeven.

Opname en transcript worden na 28 dagen vernietigd, tenzij er een bezwaar is ingediend. In het transcript wordt alleen de naam van de beller, het telefoonnummer en het onderwerp van zijn vraag vastgelegd. Als er een bezwaar wordt ingediend, wordt nog dezelfde dag doorgegeven dat de bewaartermijn verlegd moet worden.

De CPA vraagt wat er gebeurt als iemands vraag door een robot beantwoord is en er dus geen klantbeeld is gemaakt, na enige tijd weer belt met een heel ander telefoonnummer. Dan is zo iemand immers niet meer makkelijk te achterhalen. Moet hij dan alle gegevens weer helemaal opnieuw doorgeven?

Als het binnen 28 dagen gebeurt, is het betreffende gesprek alsnog handmatig terug te vinden als de beller weet hoe laat hij ongeveer gebeld heeft. Justitie dient nogal eens verzoeken in die langs deze weg gehonoreerd kunnen worden.

De CPA is benieuwd of en hoe automatische besluitvorming plaatsvindt.

Het programma handelt geen vragen af die om besluitvorming vragen en geeft alleen antwoorden op vragen om informatie. Ook vragen of men recht heeft op een bepaalde voorziening kan het programma niet beantwoorden, behalve met een doorverwijzing of –verbinding naar de betreffende dienst. Ook zullen er geen antwoorden gegenereerd worden op basis van de eigen AI in het programma.

De CPA merkt op dat in de DPIA bij de actie rond de AI-verordening geen actiehouder vermeld staat. Verder is de CPA benieuwd of overwogen is vanwege die veelheid aan verbonden applicaties voor de grondslag te verwijzen naar het register van verwerkingen. Verder hoopt de CPA dat er bij de chatbot een specifieke en makkelijk vindbare privacyverklaring komt en niet een verwijzing naar een generieke waarvoor men een aantal malen moet doorklikken.

De suggestie voor het register wordt meegenomen. Er komt een specifieke privacyverklaring.
De indieners zijn op hun beurt benieuwd of er in de aangeleverde documenten risico's gemist zijn en hoe de CPA in algemene zin kijkt naar de inzet van AI door een gemeente.

De CPA vindt dat er op zich niets mis is met de inzet van AI, maar dat het wel een grotere verantwoordelijkheid met zich meebrengt, zeker in de relatie met de burger. De keuzevrijheid van de burger is essentieel. Verhoging van de efficiency is legitiem, tenzij de overheid daardoor niet meer rechtstreeks benaderbaar is. AI biedt kansen en risico's rond privacy waar men zich bewust van dient te zijn. Dat zit onder meer in de training van de modellen, de opbrengst aan persoonsgegevens en de mogelijkheid van bias als bepaalde stemtypen niet goed herkend worden. De risico's zijn groter als een externe partij ingeschakeld wordt, omdat er dan minder toezicht is en onafhankelijkheid afneemt. Als gemeente moet je verantwoording kunnen afleggen over de herkomst van gegevens. De CPA geeft de voorkeur aan de meer transparante term algoritme boven AI.

De indieners zeggen op dezelfde lijn te zitten. Ze benadrukken dat het programma niet is opgezet met het doel geld te besparen – hooguit op IT -, maar om de dienstverlening aan de

burger te verbeteren. Voortaan zal men ook niet meer de term klant gebruiken om burgers aan te duiden.

De voorzitter bedankt voor alle toelichtingen.