Privacyoverzicht PubliekChat

Privacy vanaf het ontwerp: zo beschermt PubliekChat de gegevens van uw bezoekers

Versie 1.2 · 1 november 2026 · Policy AI Assist

Voorwoord

Inwoners en bezoekers vertrouwen erop dat een overheidsorganisatie zorgvuldig met hun gegevens omgaat. Dat vertrouwen nemen wij serieus. PubliekChat is daarom vanaf de eerste regel code gebouwd met privacy als uitgangspunt, en niet achteraf aangevuld.

Ons uitgangspunt is eenvoudig: een publieksassistent heeft geen persoonsgegevens nodig om een vraag goed te beantwoorden. Wie wil weten wanneer het zwembad open is of hoe je een vergunning aanvraagt, hoeft niet te zeggen wie hij is. Daarom zorgt PubliekChat ervoor dat persoonsgegevens zoveel mogelijk worden vervangen voordat een vraag de AI bereikt, ook als een bezoeker ze toch intypt.

In dit overzicht leest u hoe dat werkt, waar uw gegevens blijven, hoe lang ze worden bewaard en hoe PubliekChat aansluit op de AVG, de richtlijnen van de Autoriteit Persoonsgegevens en de BIO2.

1. In het kort

De belangrijkste punten

- Persoonsgegevens worden op onze eigen server zoveel mogelijk herkend en vervangen, nog voordat er iets naar de AI gaat. Daar komt geen AI aan te pas. Openbare gegevens, zoals het adres van uw organisatie, blijven gewoon staan.
- Bezoekers krijgen altijd antwoord; persoonsgegevens worden er automatisch uit gehaald.
- Vragen en antwoorden van bezoekers worden uitsluitend binnen de Europese Unie verwerkt en opgeslagen.
- AI-modellen worden niet getraind op uw gegevens of die van uw bezoekers.
- U kiest zelf hoe lang gesprekken worden bewaard: 3, 6 of 12 maanden. Uw statistieken en trends blijven 24 maanden beschikbaar.
- Logbestanden bevatten nooit de inhoud van gesprekken.
- PubliekChat is afgestemd op de AVG, het Hulpmiddel en de Handreiking generatieve AI van de Autoriteit Persoonsgegevens (juni 2026) en de BIO2.

2. Privacy vanaf het ontwerp

Waarom dit belangrijk is

De AVG vraagt organisaties om gegevensbescherming al in het ontwerp van een systeem in te bouwen (artikel 25) en niet meer gegevens te verwerken dan nodig (artikel 5 lid 1 sub c). De Autoriteit Persoonsgegevens noemt in haar Hulpmiddel voor generatieve AI uitdrukkelijk filters die persoonsgegevens tegenhouden voordat ze een AI-model bereiken. PubliekChat heeft zo'n filter standaard ingebouwd, voor elke klant en elk gesprek.

Hoe het werkt

Elke vraag gaat eerst door het privacyfilter van PubliekChat. Dat filter werkt volledig lokaal, op onze eigen server. Het gebruikt:

- vaste herkenningsregels voor bijvoorbeeld adressen, telefoonnummers en kentekens;
- rekencontroles, zoals de 11-proef voor het BSN en de officiële controles voor IBAN en creditcardnummers;
- lijsten met voornamen, achternamen en plaatsnamen, gecombineerd met de context in de zin ("mijn buurman", "mevrouw", "meneer"). Een voornaam die ook een gewoon woord is, zoals Rose of Will, wordt alleen vervangen als de zin daar aanleiding toe geeft, bijvoorbeeld bij 'ik heet'. Bekende openbare namen, zoals van bedrijven, straten, historische personen en evenementen, blijven staan zolang de vraag niet over een persoon zelf gaat. Stelt een bezoeker zich voor of noemt hij een buur, collega of kennis met zo een naam, dan wordt de naam wel vervangen.

Er gaat dus geen ruwe tekst naar een externe dienst om persoonsgegevens te herkennen. Pas als de vraag is opgeschoond, gaat hij naar de AI.

Snel én veilig

Omdat het filter op onze eigen server draait, doet het zijn werk in een fractie van een milliseconde. Bezoekers merken dus niets van de extra bescherming: ze krijgen net zo snel antwoord als zonder filter.

Ook voor anderstalige bezoekers

Het filter herkent persoonsgegevens in het Nederlands, Duits en Engels, inclusief Duitse en Belgische adressen. Zo zijn ook toeristen en internationale bezoekers beschermd. Niet alleen de nieuwe vraag gaat door het filter, maar ook eerdere berichten in hetzelfde gesprek en feedback van bezoekers.

> **Wat betekent dit voor u?**
>
> U hoeft niets in te stellen. Het privacyfilter staat standaard aan voor elke assistent en beschermt uw bezoekers vanaf het eerste gesprek.

3. Wat het filter doet

Het filter vervangt persoonsgegevens door een neutrale aanduiding. De vraag blijft daardoor begrijpelijk voor de AI, maar is veel moeilijker naar een persoon te herleiden.

Persoonsgegevens in de vraag

Gegeven	Wat er gebeurt
BSN	vervangen door [BSN]
IBAN / rekeningnummer (Nederlands en buitenlands)	vervangen door [REKENINGNUMMER]
E-mailadres	vervangen door [E-MAILADRES]
Telefoonnummer (Nederlands en buitenlands)	vervangen door [TELEFOONNUMMER]
Paspoort-, ID-kaart- of rijbewijsnummer	vervangen door [ID-DOCUMENT]
Creditcardnummer	vervangen door [CREDITCARD]
Naam	vervangen door een tijdelijk label (PERSOON_1, PERSOON_2); bekende openbare namen van bedrijven, straten, historische personen en evenementen blijven staan
Kenteken	vervangen door een tijdelijk label
IP-adres	vervangen door een tijdelijk label
Geboortedatum	voor de AI omgezet naar een leeftijd ("46 jaar"); in de opslag vervangen
Adres	volgens het adresschema hieronder
Openbare gegevens uit uw bronnen (adres en telefoonnummer van uw organisatie, namen van bestuurders, locaties)	blijven staan, zodat bezoekers ernaar kunnen vragen; een bezoeker die zich zelf met een naam of eigen adres voorstelt, wordt wel vervangen

Waarom een leeftijd in plaats van een geboortedatum?

Een geboortedatum is herleidbaar, een leeftijd veel minder. Toch kan de assistent met een leeftijd nog steeds goed antwoorden, bijvoorbeeld op de vraag of een kind van 10 jaar mee mag op een activiteit.

Adresschema

Gegeven	Vóór de AI	Vóór opslag
Straat	blijft staan	vervangen
Huisnummer (incl. toevoeging)	vervangen	vervangen
Postcode	wordt het gebiedsdeel: '1625' bij 1625 AB, en bij een buitenlandse postcode de cijfers (België, Duitsland) of het eerste deel (Verenigd Koninkrijk)	vervangen
Plaats	blijft staan	blijft staan

Waarom dit schema?

Veel vragen aan een gemeente of recreatieschap gaan over een plek: een weg die is afgesloten, een speelplaats in de buurt, de afvalinzameling in een wijk. Daarom blijven straat, plaats en de cijfers van de postcode zichtbaar voor de AI, zodat de assistent weet waar de vraag over gaat. Zonder huisnummer en zonder de letters van de postcode is een adres veel moeilijker naar één huis of persoon te herleiden. In de opslag wordt ook de straat vervangen. Zo krijgt de bezoeker een goed antwoord, terwijl er zo weinig mogelijk herleidbaars achterblijft. Het adres van uw organisatie en adressen uit uw eigen bronnen worden niet vervangen.

Tijdelijke labels, nooit opgeslagen

Namen, kentekens, IP-adressen en huisnummers krijgen een genummerd label, zoals PERSOON_1 en PERSOON_2. Zo kan de AI verschillende personen in één vraag uit elkaar houden, en blijft het antwoord begrijpelijk en persoonlijk. Alleen in het antwoord dat de bezoeker op zijn eigen scherm ziet, worden de labels teruggezet. De koppeling tussen label en gegeven bestaat uitsluitend in het werkgeheugen tijdens dat ene verzoek en wordt direct daarna weggegooid. Er wordt nergens een sleutel of koppeltabel bewaard. Nummers zoals een BSN of rekeningnummer worden nooit teruggezet: de AI heeft ze nooit nodig.

Altijd een antwoord

PubliekChat weigert geen vragen omdat er persoonsgegevens in staan. Dat is prettig voor de bezoeker, die gewoon geholpen wordt, en voor uw organisatie, omdat elke vraag meetelt in uw inzichten. De assistent laat vriendelijk weten dat persoonlijke gegevens niet nodig zijn.

Wat betekent dit voor u?

Uw bezoekers worden beschermd, ook als ze per ongeluk te veel delen. En u houdt een volledig beeld van de vragen die er leven, zonder dat u persoonsgegevens beheert.

4. Een gelaagde aanpak

Waarom meerdere lagen?

Sommige gegevens laten zich niet aan een vast patroon herkennen, zoals informatie over iemands gezondheid of persoonlijke situatie (bijzondere persoonsgegevens, AVG artikel 9). Bovendien kan een vraag over toegankelijkheid juist zo'n gegeven nodig hebben, zoals "kan ik er met een rolstoel komen?". Daarom vertrouwt PubliekChat niet op één maatregel, maar op meerdere lagen die elkaar versterken. Dat is ook de aanpak die de Autoriteit Persoonsgegevens aanbeveelt: filters, uitleg aan gebruikers en zo kort mogelijk bewaren.

De lagen:

1. Waarschuwing tijdens het typen. Typt een bezoeker een BSN, rekeningnummer, e-mailadres of telefoonnummer, dan verschijnt: "Deel liever geen persoonlijke gegevens." Versturen blijft mogelijk; de bezoeker houdt de regie.
2. Het privacyfilter. Herkent en vervangt persoonsgegevens voordat de vraag de AI bereikt.
3. Melding na het versturen. "Wij hebben persoonlijke gegevens uit uw vraag weggelaten. Die zijn niet nodig voor het antwoord." Zo weet de bezoeker precies wat er is gebeurd.
4. Vaste uitleg in de widget. "AI kan fouten maken. Deel geen persoonsgegevens."
5. Duidelijke instructies voor de AI. De assistent vraagt nooit om persoonsgegevens, herhaalt ze niet en verwijst bij een persoonlijke situatie naar het contact van uw organisatie.
6. Beperkte informatie. De AI krijgt alleen de opgeschoonde vraag en de informatie uit uw eigen bronnen, en verder niets.
7. Korte bewaartermijn. Gesprekken worden automatisch verwijderd (zie hoofdstuk 6).

Toegankelijk voor iedereen

Alle meldingen zijn gebouwd voor schermlezers. Ze worden één keer en rustig voorgelezen, en de bezoeker kan na een antwoord direct verder typen. De widget is gebouwd met WCAG 2.2 AA als doel, de toegankelijkheidsnorm voor de overheid. Een geautomatiseerde test vond geen schendingen; een formele audit door een externe partij is nog niet uitgevoerd.

> **Wat betekent dit voor u?**
>
> Bescherming die niet afhankelijk is van één maatregel, en bezoekers die begrijpen wat er met hun gegevens gebeurt. Dat draagt bij aan vertrouwen in uw dienstverlening.

5. Waar uw gegevens blijven

De onderdelen van PubliekChat die vragen en antwoorden verwerken, staan binnen de Europese Unie, bij gespecialiseerde, erkende leveranciers.

Onderdelen en locaties

Onderdeel	Wat het doet	Locatie
Applicatie	Websitewidget en beheeromgeving; verwerking van vragen, inclusief het privacyfilter	Europa
Database	Opgeschoonde gesprekken, statistieken en instellingen; versleuteld opgeslagen	Europa
AI-verwerking	Antwoorden maken en zoeken in uw bronnen, via Microsoft	EU-verwerkingszone

Geen training op uw gegevens

Microsoft gebruikt de gegevens van PubliekChat niet om AI-modellen te trainen. Wat uw bezoekers vragen, blijft van u.

Misbruikdetectie

Microsoft kan berichten tijdelijk bewaren voor misbruikdetectie. Die berichten zijn dan al door het privacyfilter op onze eigen server opgeschoond. Hier ziet u het voordeel van een lokaal filter: wat de AI-leverancier ontvangt, is al opgeschoond.

Leveranciersinformatie

Dit openbare overzicht beschrijft de aanpak zonder leveranciersnamen. Uw organisatie ontvangt na de intake een eigen dossier met de betrokken partijen, hun rol en locaties, zodat u uw eigen leveranciers- en privacybeoordeling kunt uitvoeren.

Wat betekent dit voor u?

Uw gegevens blijven binnen Europa en onder de bescherming van de AVG. Voor vragen en antwoorden van bezoekers is geen doorgifte buiten de EU nodig. Voor optionele onderdelen staan de waarborgen in uw verwerkersovereenkomst.

6. Bewaartermijnen en automatisch opruimen

Waarom dit belangrijk is

Gegevens die niet meer bestaan, kunnen ook niet uitlekken. De AVG vraagt daarom om gegevens niet langer te bewaren dan nodig (artikel 5 lid 1 sub e), en de Autoriteit Persoonsgegevens benadrukt dat dit ook geldt voor logbestanden en technische gegevens. PubliekChat ruimt daarom automatisch op.

Gegevens	Bewaartermijn
Gesprekken	u kiest zelf: 3, 6 of 12 maanden (standaard 12); daarna automatisch verwijderd
Onbeantwoorde vragen en waarderingen	zelfde termijn als gesprekken, automatisch verwijderd
Statistieken en maandrapporten	alleen opgetelde cijfers, nooit losse vragen; 24 maanden beschikbaar, ook als gesprekken eerder worden verwijderd; daarna automatisch verwijderd
Back-ups	7 dagen, daarna automatisch overschreven
Beveiligings- en controleregistratie	onveranderbaar bewaard zolang uw organisatie het platform gebruikt, zie hieronder

Alles wordt opgeslagen in de opgeschoonde versie. Bij de invoering van het nieuwe filter zijn ook alle bestaande gesprekken met dezelfde regels opgeschoond, zodat er zo min mogelijk oude persoonsgegevens achterblijven.

U houdt de regie

In het beheerpaneel kiest u zelf de bewaartermijn die past bij uw organisatie. Een kortere termijn betekent minder gegevens, zonder dat u inzicht verliest. Voordat gesprekken worden verwijderd, legt PubliekChat eerst de maandcijfers vast. Gaat daarbij iets mis, dan wordt er niets verwijderd. Zo blijven uw statistieken en trends altijd compleet.

Beveiligings- en controleregistratie

PubliekChat legt vast wie inlogt in het beheerpaneel en welke wijzigingen beheerders doen. Deze registratie is onveranderbaar, zodat niemand sporen kan wissen, ook niet iemand met toegang tot het systeem. Ze wordt bewaard zolang uw organisatie het platform gebruikt. Automatische verwijdering na beëindiging is uiterlijk 31 januari 2027 gereed; tot die tijd verwijderen wij de registratie na beëindiging op verzoek binnen 30 dagen. Het gaat alleen om gegevens van beheerders (e-mailadres, IP-adres, browser en tijdstip), nooit om gegevens van bezoekers. Doel: beveiliging en controle (AVG artikel 5 lid 1 sub e en artikel 32).

Wat betekent dit voor u?

Opslagbeperking is automatisch geregeld. U hoeft geen handmatige opschoonacties te plannen of bij te houden, en u houdt toch 24 maanden overzicht.

7. Logbestanden en monitoring

Logbestanden zijn nodig om een systeem betrouwbaar te laten werken, maar ze zijn ook een bekende plek waar persoonsgegevens ongemerkt terechtkomen. PubliekChat voorkomt dat:

- Logbestanden bevatten nooit de inhoud van gesprekken, ook niet bij foutmeldingen.
- Bestandsnamen van geüploade documenten worden niet gelogd, alleen een onherleidbare code.
- Er worden geen externe diensten voor crashrapportage gebruikt die gesprekken of gegevens kunnen ontvangen.

Dit sluit aan op BIO2-maatregel 8.15 (Logging).

8. Inzicht voor uw organisatie

Het analysedashboard en het maandrapport geven u inzicht in de vragen van uw bezoekers, zonder dat u persoonsgegevens hoeft te beheren.

Wat u ziet:

- Ontwikkeling per maand. De ontwikkeling over de afgelopen 24 maanden, met per maand een vergelijking met dezelfde maand vorig jaar. Dat werkt ook als u gesprekken na 3 of 6 maanden laat verwijderen, omdat PubliekChat alleen opgetelde cijfers bewaart en nooit losse vragen.
- Onderwerpen en trends. Waar vragen bezoekers het meest naar, en welke vragen kon de assistent nog niet beantwoorden?
- Persoonsgegevens in vragen. Hoeveel vragen persoonsgegevens bevatten en om welke soort het gaat, bijvoorbeeld namen of telefoonnummers.

Dat laatste levert twee dingen op:

- Zekerheid. U ziet met eigen ogen dat het filter zijn werk doet.
- Signalen voor uw dienstverlening. Delen bezoekers vaak hun telefoonnummer? Dan zoeken ze misschien een terugbelmogelijkheid. Noemen ze vaak hun adres? Dan leven er vragen over hun eigen buurt.

Cijfers over persoonsgegevens worden pas getoond vanaf vijf vragen, zodat niets naar een persoon te herleiden is.

> **Wat betekent dit voor u?**
>
> Volledig inzicht voor beleid en dienstverlening, met de kortst mogelijke bewaring van gesprekken. Privacy en inzicht gaan bij PubliekChat samen.

9. Onderzoek naar de gebruikte AI-modellen

Waarom dit belangrijk is

De Autoriteit Persoonsgegevens vraagt organisaties die AI inzetten om na te gaan of het gebruikte AI-model zorgvuldig is ontwikkeld (Handreiking generatieve AI, paragraaf 3.2). Voor één organisatie is dat lastig uit te zoeken. PubliekChat heeft dit onderzoek daarom voor alle klanten gedaan.

Wat wij hebben vastgesteld:

- PubliekChat gebruikt een groot taalmodel voor de antwoorden, een kleiner taalmodel voor het herkennen van onderwerpen (uitsluitend op opgeschoonde tekst) en een zoekmodel voor het doorzoeken van uw bronnen. Alle drie worden aangeboden via Microsoft, in de EU-verwerkingszone.
- De ontwikkelaar van de modellen en Microsoft hebben de gedragscode voor AI-modellen voor algemene doeleinden (GPAI Code of Practice) van de EU AI-verordening ondertekend.
- Microsoft traint geen modellen op klantgegevens.
- De bekende risico's van AI-taalmodellen, zoals onjuiste of verzonnen antwoorden, worden beperkt doordat de assistent alleen antwoordt op basis van uw eigen bronnen, zijn bronnen vermeldt en buiten zijn onderwerp niet antwoordt.

> **Wat betekent dit voor u?**
>
> U hoeft dit onderzoek niet zelf te doen. De uitkomsten staan ook in de DPIA en het ICT- en beveiligingsdocument, die het platform in het pakket Compleet automatisch voor u opstelt.

10. Getest en bewaakt

Een privacyfilter is pas waardevol als het aantoonbaar werkt. Daarom wordt het grondig getest:

- Het filter is getest met 400 verzonnen bezoekersvragen in het Nederlands, Duits en Engels, over onderwerpen als afval, vergunningen, evenementen en recreatie.
- 150 van die vragen vormen een aparte testset die niet bij de ontwikkeling van het filter is gebruikt. Daarbij is apart gemeten wat er naar de AI gaat en wat er wordt opgeslagen. Op beide momenten lagen alle categorieën binnen de gestelde grens. Een externe audit is nog niet uitgevoerd.
- Ook is getest dat openbare gegevens en bekende openbare namen blijven staan, voor onder meer een gemeente, een museum, een stichting en een bedrijf.
- Bij elke wijziging aan PubliekChat draaien alle tests automatisch opnieuw mee.
- Na elke update controleert een automatische test op de live omgeving dat een BSN nergens wordt opgeslagen.
- Ook het automatisch opruimen is getest: na het verwijderen van oude gesprekken kloppen alle maandcijfers nog tot op de laatste vraag.

11. Aansluiting op wet- en regelgeving

PubliekChat is afgestemd op de meest recente regels en richtlijnen: de AVG, het Hulpmiddel en de Handreiking generatieve AI van de Autoriteit Persoonsgegevens (juni 2026), de Baseline Informatiebeveiliging Overheid 2 (BIO2, vastgesteld in 2025 en aansluitend op ISO/IEC 27002:2022) en de EU AI-verordening.

Maatregel	AVG	Autoriteit Persoonsgegevens	BIO2 (ISO 27002:2022)
Lokaal privacyfilter vóór de AI	art. 25, art. 5 lid 1 sub c	Hulpmiddel stap 2.3 en 2.4	8.11 Maskeren van gegevens, 8.12 Voorkomen van datalekken
Bewaartermijnen en automatisch opruimen	art. 5 lid 1 sub e	Hulpmiddel stap 2.5	8.10 Verwijderen van informatie
Logbestanden zonder gespreksinhoud	art. 5 lid 1 sub c, art. 32	Hulpmiddel stap 2.5	8.15 Logging
Verwerking in de EU, geen training op klantdata	art. 28, hoofdstuk V	Hulpmiddel stap 1.4 en 2.6	5.23 Informatiebeveiliging bij clouddiensten
Onderzoek naar de AI-modellen	art. 5 lid 2	Handreiking par. 3.2	5.19 t/m 5.22 Leveranciersrelaties
Waarschuwingen en uitleg aan bezoekers	art. 12 en 13	Hulpmiddel stap 2.2	–
Input voor uw DPIA	art. 35	Hulpmiddel stap 3.1	5.34 Privacy en bescherming van persoonsgegevens

Daarnaast sluit PubliekChat aan op de EU AI-verordening: bezoekers zien altijd dat zij met een AI-assistent praten (transparantie, artikel 50).

12. Samen verantwoord

Uw organisatie blijft verantwoordelijk voor de inzet van de assistent (verwerkingsverantwoordelijke). PubliekChat neemt u daarbij zoveel mogelijk werk uit handen:

- In het pakket Compleet stelt het platform automatisch conceptdocumenten op, zoals een DPIA, een verwerkingsregister en een ICT- en beveiligingsdocument, gebaseerd op uw eigen instellingen. De verwerkersovereenkomst krijgt u in elk pakket. In het pakket Standaard helpt dit overzicht u bij het opstellen van uw eigen documenten.
- Neem de assistent op in uw verwerkingsregister. De gegevens daarvoor vindt u in het verwerkingsregister van het pakket Compleet, of in dit overzicht.
- Bekijk de inzet jaarlijks opnieuw, zoals de Autoriteit Persoonsgegevens aanbeveelt (Hulpmiddel stap 3.4).
- Zorg dat medewerkers die de assistent beheren weten hoe AI werkt (AI-geletterdheid, AI-verordening artikel 4). De handleiding in het beheerpaneel helpt daarbij.

Slot

Privacy is geen extra optie in PubliekChat, maar de basis. Zo kunt u met een gerust hart de mogelijkheden van AI benutten voor uw inwoners en bezoekers.

Vragen over privacy? Neem contact op met Policy AI Assist via hallo@publiekchat.nl.

Versiegeschiedenis

Versie	Datum	Wijziging
1.2	1 november 2026	Bekende openbare namen blijven staan, postcodetabel aangevuld.
1.1	31 oktober 2026	Openbare gegevens blijven staan, postcodes per land, bewaartermijn registraties, testmethode, toegankelijkheid, pakketten.
1.0	26 oktober 2026	Eerste versie.