

Security- en privacyoverzicht

Klantvriendelijke uitleg van de standaard beveiligings- en privacymaatregelen

Versie 1.0 | 7 september 2026

In één zin

AI Reception verwerkt alleen de informatie die nodig is om gesprekken af te handelen, beschermt beheeraccounts met MFA en bewaart klantinhoud in het beheerde dashboard standaard maximaal 30 dagen.

1. Onze standaardmaatregelen

Onderwerp	Wat wij toepassen
AI-transparantie	De beller hoort aan het begin dat hij of zij met een AI-assistent spreekt.
MFA	Meervoudige verificatie is verplicht voor beheeraccounts waar de leverancier dit ondersteunt.
Persoonlijke toegang	Unieke accounts, geen gedeelde beheerlogins en minimaal noodzakelijke rechten.
Veilige verbindingen	HTTPS/TLS voor website, API- en dashboardverkeer waar ondersteund.
Webhookcontrole	Authenticatie van inkomende systeemmeldingen met secrets/tokens en validatie.
Datascheiding	Klantdata wordt logisch gescheiden en alleen zichtbaar voor bevoegde gebruikers.
Bewaring	Klantinhoud standaard maximaal 30 dagen; kortere termijn mogelijk.
Opnames	Niet standaard nodig. Alleen activeren na duidelijke afspraak, doel en informatie aan bellers.
Monitoring	Technische fouten, verdachte toegang en belangrijke wijzigingen worden gevolgd en onderzocht.
Incidentrespons	Vast proces voor containment, onderzoek, klantmelding, herstel en evaluatie.

2. Welke gegevens kunnen worden verwerkt?

- Naam, telefoonnummer en eventueel e-mailadres of adres.
- Bestelling, reservering, afspraak, terugbelverzoek of andere klantvraag.

- Gespreksmetadata zoals tijdstip, duur en status.
- Transcript of samenvatting wanneer dit voor de gekozen dienst nodig is.
- Gespreksopname uitsluitend wanneer de klant dit expliciet laat activeren.

Niet bedoeld voor gevoelige gegevens

Volledige betaalkaartgegevens en bijzondere persoonsgegevens horen niet in de standaard AI-telefonieflow. Voor zorg, juridische dossiers, biometrie of andere gevoelige sectoren is vooraf een aparte risico- en compliancebeoordeling nodig.

3. Bewaartermijn en verwijderen

Klantinhoud in het door ons beheerde dashboard wordt standaard uiterlijk na 30 dagen verwijderd. Sommige leveranciers verwijderen call-artefacten eerder. Bij beëindiging verwijderen we de actieve klantomgeving binnen maximaal 30 dagen nadat een eventuele export is afgerond. Wettelijk noodzakelijke factuur- of minimale beveiligingsmetadata kan apart langer worden bewaard zonder onnodige gespreksinhoud.

4. Leveranciers en opslaglocaties

We gebruiken gespecialiseerde leveranciers. Niet iedere leverancier is voor iedere klant actief. Omdat voice-AI en telefonie soms buiten de EER worden verwerkt, publiceren we een apart leveranciersregister met functie, status, mogelijke locatie, bewaartermijn en waarborgen. De klantspecifieke bijlage vermeldt de werkelijk geactiveerde leveranciers.

5. Wat gebeurt er bij een incident?

1. We stoppen of beperken het incident en beveiligen accounts, tokens en koppelingen.
2. We onderzoeken welke klant, systemen en gegevens zijn geraakt.
3. Bij een bevestigd incident met persoonsgegevens informeren we de klant zonder onnodige vertraging; streeftijd binnen 24 uur na bevestiging waar haalbaar.
4. We werken mee aan herstel, documentatie en een eventuele melding aan de Autoriteit Persoonsgegevens.
5. Na afloop voeren we verbetermaatregelen uit en leggen we de beslissing vast.

6. Gedeelde verantwoordelijkheid

AI Reception	De klant
Beveiligt de technische dienst, beheeraccounts, koppelingen en leveranciersconfiguratie.	Levert correcte bedrijfsinformatie, bepaalt doel en grondslag en informeert eigen klanten/bellers.
Ondersteunt verwijderverzoeken en incidentonderzoek.	Beheert wie toegang krijgt tot tablet/dashboard en meldt verloren apparaten of vertrekkende medewerkers.
Documenteert leveranciers, bewaring en standaardmaatregelen.	Geeft geen bijzondere persoonsgegevens of betaalkaartgegevens door zonder aparte afspraken.

7. Downloadbare documenten

- Modelverwerkersovereenkomst (in te vullen en te ondertekenen per klant).
- Leveranciers- en opslaglocatieregister.
- Verwijderingsprocedure.
- Incident-responseprocedure.

Privacy- of beveiligingsvraag?

Neem contact op via info@aireception.nl of 065 791 20 71. Vermeld de bedrijfsnaam en, indien beschikbaar, een call-ID of datum/tijdstip. Deel geen wachtwoorden, API-keys of volledige gevoelige klantgegevens per e-mail.

Bronnen en externe documentatie

De onderstaande bronnen zijn gebruikt om de juridische en technische beschrijvingen te controleren. Leveranciers kunnen hun voorwaarden en infrastructuur wijzigen; controleer de actuele versie bij contractering.

- European Commission - Standard contractual clauses between controllers and processors: https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en
- European Data Protection Board - Data breach guidance for small businesses: https://www.edpb.europa.eu/sme/assess-the-risks/data-breaches_en
- Autoriteit Persoonsgegevens - Datalek: dit moet u doen: <https://autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-dit-moet-u-doen>
- Vapi call retention documentation: <https://docs.vapi.ai/assistants/call-recording>
- OpenAI API data controls: <https://platform.openai.com/docs/models/default-usage-policies-by-endpoint>