

Modelverwerkersovereenkomst

Concept voor de verwerking van persoonsgegevens bij AI-telefonie, dashboards en meldingen

Versie 1.0 | 7 september 2026

Belangrijk

Dit is een professioneel conceptmodel en geen individueel juridisch advies. Vul de juridische naam, het adres, het KvK-nummer, de klantgegevens, de exacte leveranciers en de gekozen technische configuratie in voordat partijen ondertekenen. Laat het model juridisch controleren wanneer de verwerking gevoelig, grootschalig of sectorspecifiek is.

Partijen

Rol	Partijgegevens
Verwerkingsverantwoordelijke (klant)	[Officiële bedrijfsnaam klant] [Adres] [KvK-nummer] [Contactpersoon en e-mail]
Verwerker	[Juridische naam achter AI Reception] Handelsnaam: AI Reception / aireception.nl [Adres en vestigingsplaats] KvK: [in te vullen] E-mail: info@aireception.nl

1. Onderwerp en toepasselijkheid

Deze overeenkomst regelt de verwerking van persoonsgegevens door Verwerker namens Verwerkingsverantwoordelijke in het kader van de AI Reception-dienst. De commerciële hoofdovereenkomst, orderbevestiging en deze verwerkersovereenkomst vormen samen de afspraken tussen partijen. Bij tegenstrijdigheid over persoonsgegevens gaat deze verwerkersovereenkomst voor, tenzij schriftelijk anders overeengekomen.

2. Duur

De overeenkomst gaat in op de startdatum van de dienst en blijft van kracht zolang Verwerker persoonsgegevens namens Verwerkingsverantwoordelijke verwerkt. Na beëindiging worden persoonsgegevens verwijderd of teruggegeven volgens artikel 13 en de geldende bewaartermijnen, behoudens een wettelijke verplichting om bepaalde gegevens langer te bewaren.

3. Aard en doel van de verwerking

- Telefonische oproepen ontvangen en laten afhandelen door een AI-assistent.
- Vragen beantwoorden op basis van door de klant aangeleverde bedrijfsinformatie.

- Bestellingen, reserveringen, afspraken en terugbelverzoeken registreren.
- Gesprekssamenvattingen, statussen en meldingen beschikbaar stellen in een dashboard of notificatiekanaal.
- Telefonie, dashboards, tablet- of kassaworkflows technisch beheren, beveiligen, testen en ondersteunen.

AI-transparantie

De beller wordt bij aanvang duidelijk geïnformeerd dat hij of zij met een AI-assistent spreekt. De AI mag geen informatie verzinnen en moet bij onzekerheid escaleren, doorverbinden of een terugbelverzoek registreren volgens de instructies van de klant.

4. Categorieën betrokkenen en persoonsgegevens

Categorie	Voorbeelden
Betrokkenen	Bellers, klanten, potentiële klanten, leveranciers/contactpersonen en medewerkers die als doorverbind- of meldingscontact zijn opgegeven.
Identificatie- en contactgegevens	Naam, telefoonnummer, e-mailadres, adres of afleveradres.
Dienst- en transactiegegevens	Bestelling, reservering, afspraak, voertuiggegevens, voorkeuren, opmerkingen en status.
Communicatiegegevens	Gespreksmetadata, transcript of samenvatting; opname uitsluitend indien expliciet geactiveerd.
Technische gegevens	Tijdstip, gespreksduur, call-ID, apparaat-/dashboardlog en foutinformatie.

Bijzondere persoonsgegevens

De standaarddienst is niet bedoeld voor medische gegevens, strafrechtelijke gegevens, volledige betaalkaartgegevens of andere bijzondere persoonsgegevens. Zulke verwerking is alleen toegestaan na een aparte schriftelijke risicoanalyse, passende contracten en aanvullende technische maatregelen.

5. Verwerking uitsluitend op instructie

Verwerker verwerkt persoonsgegevens uitsluitend op gedocumenteerde instructies van Verwerkingsverantwoordelijke, waaronder de intake, systeemconfiguratie, goedgekeurde scripts, kennisbank, openingstijden, doorverbindregels en schriftelijke wijzigingsverzoeken. Wanneer een instructie naar het redelijke oordeel van Verwerker in strijd is met toepasselijke privacywetgeving, meldt Verwerker dit en schort hij de betreffende handeling op totdat partijen duidelijkheid hebben.

6. Geheimhouding en medewerkers

- Toegang is beperkt tot personen die deze voor hun taak nodig hebben.
- Bevoegde personen zijn gebonden aan vertrouwelijkheid.
- Beheeraccounts zijn persoonlijk; gedeelde beheerlogins zijn niet toegestaan.
- Toegang wordt ingetrokken wanneer een rol eindigt of niet langer nodig is.

7. Technische en organisatorische maatregelen

Maatregel	Standaardbeleid
Toegangsbeveiliging	MFA voor beheeraccounts, unieke accounts, sterke wachtwoorden en minimaal noodzakelijke rechten.
Transportbeveiliging	TLS/HTTPS voor webverkeer en API-koppelingen waar ondersteund.
Webhook-beveiliging	Authenticatie met secrets/tokens, validatie van herkomst en beperking van toegestane acties.
Datascheiding	Klantdata logisch gescheiden via klant-, organisatie- of account-ID en autorisatieregels.
Bewaartermijn	Klantinhoud in het beheerde dashboard standaard maximaal 30 dagen; leveranciers kunnen bepaalde artefacten eerder verwijderen.
Opnames	Gespreksopname standaard uit, tenzij schriftelijk nodig en geactiveerd met passende informatie aan betrokkenen.
Monitoring	Fout- en beveiligingsmonitoring, incidentregistratie en periodieke beoordeling van toegangsrechten.
Continuïteit	Herstelprocedures, leveranciersmonitoring en waar passend back-ups zonder onnodige klantinhoud.

8. Subverwerkers

Verwerkingsverantwoordelijke verleent algemene toestemming voor het gebruik van subverwerkers die nodig zijn voor telefonie, AI, spraak, hosting, e-mail en notificaties, mits deze zijn opgenomen in het actuele leveranciersregister of een klantspecifieke bijlage. Verwerker meldt materiële wijzigingen vooraf binnen een redelijke termijn. De klant kan gemotiveerd bezwaar maken wanneer een nieuwe subverwerker een aantoonbaar privacy- of beveiligingsrisico oplevert. Verwerker legt aan subverwerkers passende gegevensbeschermingsverplichtingen op.

9. Internationale doorgifte

Sommige leveranciers verwerken gegevens buiten de Europese Economische Ruimte. In dat geval wordt een geldige doorgiftegrondslag gebruikt, zoals een adequaatheidsbesluit, het EU-US Data Privacy Framework waar toepasselijk, of door de Europese Commissie vastgestelde Standard Contractual Clauses met aanvullende maatregelen waar nodig. De exacte doorgifte en opslaglocatie wordt in het leveranciersregister en de klantspecifieke configuratie beschreven.

10. Rechten van betrokkenen

Verwerker ondersteunt Verwerkingsverantwoordelijke redelijkerwijs bij verzoeken om inzage, correctie, verwijdering, beperking, bezwaar en dataportabiliteit. Verwerker reageert niet zelfstandig inhoudelijk op een verzoek van een beller, tenzij de klant dit uitdrukkelijk opdraagt of de wet dit vereist. Een ontvangen verzoek wordt zonder onnodige vertraging doorgestuurd naar de aangewezen contactpersoon van de klant.

11. DPIA, toezicht en informatieplicht

Verwerker verstrekt beschikbare informatie die redelijkerwijs nodig is voor een gegevensbeschermingseffectbeoordeling, voorafgaande raadpleging of controle door een toezichthouder. De klant blijft verantwoordelijk voor de rechtmatigheid van de verwerking, de informatie aan bellers, de gekozen doeleinden, de inhoud van de kennisbank en het bepalen of een DPIA vereist is.

12. Beveiligingsincidenten en datalekken

Verwerker meldt een bevestigd incident met persoonsgegevens zonder onnodige vertraging aan de klant via het afgesproken contactpunt. De streeftijd is binnen 24 uur na bevestiging, voor zover de beschikbare informatie dit toelaat. De melding bevat waar mogelijk de aard en omvang, betrokken gegevenscategorieën, vermoedelijke gevolgen, genomen maatregelen en een contactpunt. Verwerker werkt mee aan onderzoek, beperking, herstel en documentatie. De klant beoordeelt of melding aan de Autoriteit Persoonsgegevens en/of betrokkenen nodig is.

13. Verwijdering en teruggave

- Klantinhoud in het dashboard wordt standaard uiterlijk na 30 dagen verwijderd, tenzij een kortere termijn is ingesteld of een wettelijke uitzondering geldt.
- Na beëindiging verwijdert Verwerker de actieve klantconfiguratie en klantinhoud binnen 30 dagen, tenzij de klant vooraf om export of eerdere verwijdering vraagt.
- Gegevens bij subverwerkers worden verwijderd via de beschikbare beheer- of supportprocedures; technische back-ups verlopen volgens de leverancier en worden niet voor normaal gebruik teruggezet.
- Minimale factuur-, contract- en beveiligingsmetadata kan langer worden bewaard wanneer de wet of de bescherming van rechtsvorderingen dit vereist; gespreksinhoud wordt daarvan gescheiden.

14. Controle en bewijs

Verwerker stelt op verzoek relevante documentatie beschikbaar, zoals dit contract, het leveranciersregister, een beschrijving van beveiligingsmaatregelen en beschikbare certificeringen of verklaringen van leveranciers. Een audit vindt plaats met redelijke aankondiging, tijdens kantooruren, met bescherming van vertrouwelijke gegevens van andere klanten en voor rekening van de verzoekende partij, tenzij de audit nodig is vanwege een aan Verwerker toerekenbaar ernstig incident.

15. Slotbepalingen

- Nederlands recht is van toepassing, tenzij de hoofdovereenkomst rechtsgeldig anders bepaalt.
- Wijzigingen zijn alleen geldig wanneer deze schriftelijk of elektronisch zijn vastgelegd.
- De aansprakelijkheidsregeling uit de hoofdovereenkomst geldt, voor zover wettelijk toegestaan.
- Wanneer een bepaling ongeldig blijkt, blijven de overige bepalingen van kracht.

Bijlage A - Details van de verwerking

Onderdeel	In te vullen / standaard
Startdatum	[datum]
Duur	Looptijd van de AI Reception-dienst plus verwijderperiode.
Doel	Telefonische klantafhandeling, registratie, dashboard en meldingen.
Categorieën betrokkenen	Bellers, klanten, medewerkers en zakelijke contactpersonen.
Gegevens	Contactgegevens, aanvraag-/order-/afspraakgegevens, callmetadata en alleen indien geactiveerd transcript/opname.
Bewaartermijn klantinhoud	Standaard maximaal 30 dagen.
Meldingscontact klant	[naam, telefoon, e-mail]
Toegestane talen en use-cases	[invullen]
Verboden gegevens/use-cases	Bijzondere persoonsgegevens en volledige betaalkaartgegevens, tenzij apart overeengekomen.

Bijlage B - Klantspecifieke technische configuratie

Onderdeel	Keuze
Opname	☐ Uit (standaard) ☐ Aan, met grondslag/informatie: _____
Transcript	☐ Uit ☐ Aan
Dashboardbewaring	☐ 7 dagen ☐ 14 dagen ☒ 30 dagen ☐ Anders: ____
Notificaties	☐ Dashboard ☐ Tablet ☐ WhatsApp ☐ SMS ☐ E-mail
Doorverbinden	☐ Nee ☐ Ja, naar: _____
Opslagregio/leveranciers	Zie klantspecifieke leveranciersbijlage.

Bijlage C - Subverwerkers

Het actuele document “Leveranciers en opslaglocaties” maakt deel uit van deze overeenkomst. Alleen de leveranciers die voor deze klant daadwerkelijk zijn geactiveerd gelden als subverwerker voor de betreffende dienst.

Ondertekening

Verwerkingsverantwoordelijke	Verwerker
Naam: _____	Juridische naam: _____
Functie: _____	Naam: _____
Datum: _____	Datum: _____
Handtekening: _____	Handtekening: _____

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>