Verwerkersovereenkomst Boekenbloom

Versie 1.3 · ingangsdatum: 8 november 2026

Vervangt versie 1.0. Klinieken die eerder een versie hebben aanvaard, aanvaarden deze versie bij hun volgende login.

Deze verwerkersovereenkomst wordt gesloten tussen:

1. De klant: de onderneming die zich registreert op het platform van Boekenbloom en deze overeenkomst elektronisch aanvaardt, vertegenwoordigd door de persoon die de aanvaarding verricht (hierna: "Verwerkingsverantwoordelijke"); en
2. Boeken Bloom B.V., gevestigd aan Barajasweg 82, 1043 CP Amsterdam, ingeschreven bij de Kamer van Koophandel onder nummer 42153269 (hierna: "Verwerker").

1. Onderwerp, duur en rolverdeling

1.1 Verwerker levert een online platform voor het plannen van afspraken, een agenda, klantcommunicatie per e-mail en sms, een AI-boekingsassistent (webchat), reviews van klanten, het beheren van advertentiecampagnes en het meten van de resultaten daarvan (de "Dienst"). Daarbij verwerkt Verwerker persoonsgegevens in opdracht van Verwerkingsverantwoordelijke. Bijlage 1 beschrijft de verwerkingen.

1.2 Verwerkingsverantwoordelijke bepaalt het doel en de middelen van de verwerking van persoonsgegevens van haar klanten en potentiële klanten. Verwerker is voor deze verwerkingen verwerker in de zin van artikel 28 AVG.

1.3 Deze overeenkomst geldt niet voor verwerkingen waarvoor Verwerker zelf verwerkingsverantwoordelijke is, zoals het beheer van kliniekaccounts, facturatie, beveiliging van het platform en de eigen website van Verwerker. Daarvoor geldt de privacyverklaring van Verwerker.

1.4 Deze overeenkomst geldt zolang Verwerker persoonsgegevens verwerkt voor Verwerkingsverantwoordelijke en maakt deel uit van de afspraken over het gebruik van de Dienst.

2. Aard, doel en gegevens

2.1 De doeleinden, categorieën betrokkenen en categorieën persoonsgegevens staan in Bijlage 1.

2.2 Verwerkingsverantwoordelijke legt in de Dienst geen bijzondere categorieën van persoonsgegevens vast als bedoeld in artikel 9 AVG, in het bijzonder geen gegevens over gezondheid (zoals aandoeningen, allergieën, medicatie of medische voorgeschiedenis), en vraagt betrokkenen niet om zulke gegevens via de Dienst te verstrekken, waaronder het opmerkingenveld bij een afspraak, de interne notities, de webchat en reviews. Zulke gegevens horen in het eigen (medisch) dossier van Verwerkingsverantwoordelijke.

2.3 De naam van een gekozen behandeling kan in bepaalde gevallen indirect iets zeggen over de gezondheid van een betrokkene. Verwerker gebruikt deze uitsluitend voor het plannen en beheren van de afspraak en neemt deze niet op in gegevens die naar advertentieplatforms worden verzonden, ook niet via webadressen of paginatitels. Verwerkingsverantwoordelijke draagt er zorg voor dat voor deze verwerking een geldige grondslag bestaat.

2.4 Verwerker wijst betrokkenen erop geen medische gegevens te delen (bij het opmerkingenveld, in het eerste antwoord van de webchat en in het reviewformulier), beperkt de lengte van vrije tekstvelden en laat de AI-boekingsassistent niet naar gezondheidsgegevens vragen. Medische vragen worden doorgezet naar Verwerkingsverantwoordelijke. Reviews worden vóór publicatie automatisch gecontroleerd op mogelijke gezondheidsgegevens en zo nodig door een medewerker van Verwerker beoordeeld. Ontvangt Verwerker desondanks bijzondere persoonsgegevens, dan verwerkt Verwerker deze niet verder dan nodig is voor het

uitvoeren van de Dienst, deelt Verwerker deze niet met advertentieplatforms, publiceert Verwerker deze niet en verwijdert Verwerker deze op verzoek van Verwerkingsverantwoordelijke.

3. Instructies van Verwerkingsverantwoordelijke

3.1 Verwerker verwerkt persoonsgegevens uitsluitend op basis van schriftelijke instructies van Verwerkingsverantwoordelijke, ook wat betreft doorgifte naar landen buiten de EER, tenzij een wettelijke verplichting anders vereist. In dat geval informeert Verwerker Verwerkingsverantwoordelijke vooraf, tenzij de wet dat verbiedt.

3.2 Deze overeenkomst, de algemene voorwaarden (waaronder de reviewregels) en de instellingen die Verwerkingsverantwoordelijke in de Dienst kiest (zoals het aanzetten van de webchat, reviews of sms-herinneringen en het koppelen van een advertentieaccount) gelden als schriftelijke instructies.

3.3 Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk in kennis als een instructie naar zijn oordeel inbreuk maakt op de AVG of andere regels over gegevensbescherming.

4. Advertentiemeting

4.1 Koppelt Verwerkingsverantwoordelijke een eigen advertentieaccount aan de Dienst (zoals Google Ads, en wanneer beschikbaar TikTok of een Meta-dataset), dan geeft zij Verwerker de instructie om boekingsgebeurtenissen namens haar naar dat account te verzenden, uitsluitend onder de voorwaarden van dit artikel.

4.2 Verwerker verzendt een boekingsgebeurtenis alleen als de betrokkene daarvoor vooraf, vrij, specifiek en ondubbelzinnig toestemming heeft gegeven via een niet vooraf aangevinkt vakje, waarin de platforms worden genoemd waaraan de gegevens worden doorgegeven. De aanwezigheid van een advertentie-klik-ID of een advertentiecookie geldt niet als toestemming. Verwerker legt per boeking vast of en wanneer toestemming is gegeven en welke versie van de toestemmingstekst is getoond.

4.3 Verwerker verzendt per gebeurtenis alleen: een boekings-ID, het tijdstip, het type gebeurtenis, het e-mailadres en telefoonnummer uitsluitend in gehashte vorm (SHA-256), advertentie-identificatoren (zoals gclid, ttclid, fbclid en advertentiecookies), en bij websiteboekingen IP-adres en browsertype en het webadres zonder pad en parameters. Verwerker verzendt nooit de gekozen behandeling, opmerkingen, naam, chatberichten of reviews.

4.4 Trekt de betrokkene de toestemming in, dan verzendt Verwerker vanaf dat moment geen gebeurtenissen meer over die betrokkene. Eerder verzonden gegevens vallen onder de verantwoordelijkheid van Verwerkingsverantwoordelijke en het betreffende platform.

4.5 Advertentieplatforms zijn voor deze verzending geen subverwerkers van Verwerker. Zij ontvangen de gegevens op grond van de overeenkomsten die Verwerkingsverantwoordelijke zelf met hen heeft gesloten (zoals de gegevensverwerkingsvoorwaarden van Google Ads). Verwerkingsverantwoordelijke is ervoor verantwoordelijk dat deze overeenkomsten zijn aanvaard en dat haar eigen privacyverklaring deze verwerking vermeldt.

4.6 Op de boekingspagina laadt Verwerker advertentiecookies of pixels van Verwerkingsverantwoordelijke pas na toestemming voor marketingcookies, met uitgeschakelde automatische gegevensverzameling.

5. Geheimhouding en beveiliging

5.1 Verwerker zorgt dat personen die toegang hebben tot de persoonsgegevens gebonden zijn aan geheimhouding.

5.2 Verwerker neemt passende technische en organisatorische maatregelen als bedoeld in artikel 32 AVG.

Bijlage 3 beschrijft de maatregelen.

6. Subverwerkers

6.1 Verwerkingsverantwoordelijke geeft algemene schriftelijke toestemming voor de inzet van de subverwerkers in Bijlage 2.

6.2 Verwerker informeert Verwerkingsverantwoordelijke ten minste 14 dagen vooraf per e-mail over een nieuwe of vervangende subverwerker. Verwerkingsverantwoordelijke kan binnen die termijn op redelijke gronden bezwaar maken. Komen partijen er niet uit, dan kan Verwerkingsverantwoordelijke de overeenkomst kosteloos opzeggen.

6.3 Verwerker legt subverwerkers ten minste gelijkwaardige verplichtingen op als in deze overeenkomst en blijft tegenover Verwerkingsverantwoordelijke verantwoordelijk voor de nakoming daarvan.

7. Doorgifte buiten de EER

7.1 Verwerker slaat de gegevens van de Dienst op in de EER. Doorgifte buiten de EER vindt alleen plaats aan de subverwerkers in Bijlage 2 en alleen met passende waarborgen, zoals een adequaatheidsbesluit (waaronder het EU-VS Data Privacy Framework) of standaardcontractbepalingen van de Europese Commissie.

8. Rechten van betrokkenen en bijstand

8.1 Verwerker ondersteunt Verwerkingsverantwoordelijke, voor zover redelijk, bij het beantwoorden van verzoeken van betrokkenen (zoals inzage, correctie, verwijdering en intrekking van toestemming). Ontvangt Verwerker zo'n verzoek rechtstreeks, dan stuurt Verwerker het binnen 5 werkdagen door.

8.2 Verwerker ondersteunt Verwerkingsverantwoordelijke, voor zover redelijk, bij de verplichtingen uit de artikelen 32 tot en met 36 AVG, waaronder een gegevensbeschermingseffectbeoordeling (DPIA), door de benodigde informatie over de Dienst te verstrekken.

9. Datalekken

9.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging, en uiterlijk binnen 24 uur na ontdekking, over een inbreuk in verband met persoonsgegevens.

9.2 Verwerker verstrekt daarbij, voor zover bekend: de aard van de inbreuk, de categorieën en het geschatte aantal betrokkenen en gegevens, de waarschijnlijke gevolgen, de genomen en voorgestelde maatregelen en een contactpersoon. Verwerkingsverantwoordelijke beslist over een melding aan de Autoriteit Persoonsgegevens en betrokkenen.

10. Controle

10.1 Verwerker stelt op verzoek de informatie beschikbaar die nodig is om naleving van deze overeenkomst aan te tonen. Een audit door een onafhankelijke deskundige met geheimhoudingsplicht is mogelijk na redelijke aankondiging, maximaal eenmaal per jaar, op kosten van Verwerkingsverantwoordelijke.

11. Bewaren en verwijderen

11.1 Verwerker bewaart persoonsgegevens niet langer dan nodig voor de Dienst, volgens de termijnen in Bijlage 1, tenzij Verwerkingsverantwoordelijke een kortere termijn instelt.

11.2 Na beëindiging van de Dienst verwijdert Verwerker de persoonsgegevens binnen 30 dagen, of geeft deze op verzoek vooraf terug in een gangbaar formaat, tenzij een wettelijke bewaarplicht geldt. Back-ups

worden binnen de gebruikelijke rotatie (maximaal 30 dagen daarna) overschreven.

12. Aansprakelijkheid

12.1 De aansprakelijkheid van partijen onder deze overeenkomst volgt de afspraken over aansprakelijkheid in de algemene voorwaarden van Verwerker. Elke partij is tegenover betrokkenen en toezichthouders verantwoordelijk volgens artikel 82 en 83 AVG.

12.2 Verwerkingsverantwoordelijke vrijwaart Verwerker voor aanspraken van derden die het gevolg zijn van onrechtmatige instructies van Verwerkingsverantwoordelijke, het ontbreken van een grondslag die zij moest hebben, of het vastleggen van bijzondere persoonsgegevens in strijd met artikel 2.2.

13. Slotbepalingen

13.1 Op deze overeenkomst is Nederlands recht van toepassing. Geschillen worden voorgelegd aan de bevoegde rechter te Amsterdam.

13.2 Verwerker kan deze overeenkomst wijzigen. Een nieuwe versie wordt ter aanvaarding voorgelegd; tot aanvaarding blijft de vorige versie gelden.

13.3 Deze overeenkomst wordt elektronisch aanvaard. Verwerker registreert de naam en functie van de ondertekenaar, de onderneming, het KvK-nummer, de versie, datum en tijd en het IP-adres van de aanvaarding.

Bijlage 1: Verwerkingen

Afspraken plannen en beheren (agenda), bevestigingen, herinneringen per e-mail en sms

- Betrokkenen: Klanten van Verwerkingsverantwoordelijke
- Persoonsgegevens: Naam, e-mail, telefoon, taal, behandeling, datum/tijd, medewerker, opmerkingen (max. 300 tekens), interne notities, status (zoals afgerond of niet verschenen), privacy- en marketingkeuze
- Bewaartermijn (standaard): Zolang de kliniek de Dienst gebruikt; afgelopen en geannuleerde afspraken uiterlijk 24 maanden na de afspraakdatum

AI-boekingsassistent (webchat) op de boekingspagina, een chatpagina of de website van de kliniek

- Betrokkenen: Klanten en potentiële klanten
- Persoonsgegevens: Chatberichten, opgegeven naam en contactgegevens, gekozen afspraak, advertentieverwijzing van de pagina; gehasht IP-adres voor misbruikbeperking
- Bewaartermijn (standaard): Gesprekken 12 maanden na het laatste bericht; gehasht IP-adres maximaal 7 dagen

Reviews (als de kliniek deze aanzet): uitnodiging na een afgeronde afspraak, plaatsen, controleren en tonen

- Betrokkenen: Klanten met een afgeronde afspraak
- Persoonsgegevens: E-mailadres (voor de uitnodiging), beoordeling, reviewtekst, weergavenaam (voornaam + initiaal), datum, reactie van de kliniek, meldingen
- Bewaartermijn (standaard): Reviewtekst 24 maanden na publicatie; beoordeling, datum en weergavenaam zolang de kliniek de Dienst gebruikt

Meldingen aan de kliniek (e-mail)

- Betrokkenen: Klanten; medewerkers van de kliniek
- Persoonsgegevens: Afspraakgegevens; naam en contactgegevens van medewerkers
- Bewaartermijn (standaard): Als afspraken

Medewerkers en beschikbaarheid

- Betrokkenen: Medewerkers van de kliniek

Persoonsgegevens: Naam, functie, werktijden, diensten

Bewaartermijn (standaard): Zolang de kliniek de Dienst gebruikt

Advertentiemeting (artikel 4)

Betrokkenen: Klanten die toestemming gaven

Persoonsgegevens: Boekings-ID, gehasht e-mailadres en telefoonnummer, klik-ID's, IP-adres, browser, tijdstip

Bewaartermijn (standaard): Verzendlog: 90 dagen

Campagnebeheer en kostenrapportage

Betrokkenen: n.v.t.

Persoonsgegevens: Geaggregeerde advertentiekosten en resultaten, geen persoonsgegevens van klanten

Bewaartermijn (standaard): Zolang de kliniek de Dienst gebruikt

Bijlage 2: Subverwerkers

Supabase Inc.

Doel: Database, authenticatie, opslag

Locatie gegevens: EU (Ierland)

Waarborg bij doorgifte: Standaardcontractbepalingen voor eventuele toegang vanuit de VS

Vercel Inc.

Doel: Hosting van de applicatie

Locatie gegevens: VS (verwerking), opslag in de database in de EU

Waarborg bij doorgifte: EU-VS Data Privacy Framework / standaardcontractbepalingen

Resend Inc.

Doel: Verzenden van e-mail

Locatie gegevens: VS

Waarborg bij doorgifte: Standaardcontractbepalingen

CM.com Netherlands B.V.

Doel: Verzenden van sms-herinneringen (als de kliniek dit aanzet)

Locatie gegevens: NL/EU

Waarborg bij doorgifte: n.v.t.

Anthropic PBC

Doel: AI-boekingsassistent (webchat) en automatische controle van reviews

Locatie gegevens: VS

Waarborg bij doorgifte: EU-VS Data Privacy Framework / standaardcontractbepalingen

Cloudflare Inc.

Doel: Botbescherming (Turnstile) bij de webchat

Locatie gegevens: EU/VS

Waarborg bij doorgifte: EU-VS Data Privacy Framework / standaardcontractbepalingen

TransIP B.V.

Doel: Domein en e-mail van Boekenbloom

Locatie gegevens: NL

Waarborg bij doorgifte: n.v.t.

Advertentieplatforms zijn geen subverwerkers: zie artikel 4.5.

Bijlage 3: Beveiligingsmaatregelen

- Versleuteling van gegevens tijdens transport (TLS) en opslag.
- Toegangsbeperking per kliniek op databaseniveau (row level security); medewerkers van een kliniek zien alleen gegevens van die kliniek.
- Beheerderstoegang van Boekenbloom alleen met persoonlijke accounts en tweestapsverificatie (TOTP); acties van beheerders worden gelogd.
- Geheime sleutels (zoals advertentietokens) worden versleuteld opgeslagen en zijn na invoer niet meer leesbaar in het dashboard.
- Pseudonimisering (SHA-256) van e-mailadres en telefoonnummer vóór verzending naar advertentieplatforms; IP-adressen voor misbruikbeperking alleen gehasht.
- Botbescherming en limieten per sessie en per kliniek op registratie, inloggen en de webchat.
- Dataminimalisatie: beperkte vrije tekstvelden, waarschuwing tegen medische gegevens, geen behandeling in advertentiegegevens, controle van reviews vóór publicatie.
- Automatische verwijdering volgens de bewaartermijnen in Bijlage 1.
- Back-ups volgens de voorzieningen van de databaseleverancier.
- Beleid voor het melden en afhandelen van beveiligingsincidenten binnen 24 uur.