Boekenbloom Data Processing Agreement

Version 1.3 · effective date: 8 November 2026

Replaces version 1.0. Clinics that accepted an earlier version accept this version at their next login.

This is a translation; the Dutch version prevails.

This data processing agreement is entered into between:

1. The customer: the business that registers on the Boekenbloom platform and accepts this agreement electronically, represented by the person who performs the acceptance (hereinafter: "Controller"); and
2. Boeken Bloom B.V., located at Barajasweg 82, 1043 CP Amsterdam, registered with the Dutch Chamber of Commerce under number 42153269 (hereinafter: "Processor").

1. Subject, duration and roles

1.1 Processor provides an online platform for scheduling appointments, a calendar, customer communication by email and SMS, an AI booking assistant (web chat), customer reviews, managing advertising campaigns and measuring their results (the "Service"). In doing so, Processor processes personal data on behalf of Controller. Annex 1 describes the processing.

1.2 Controller determines the purpose and means of the processing of personal data of its customers and potential customers. Processor is a processor within the meaning of article 28 GDPR for this processing.

1.3 This agreement does not apply to processing for which Processor is itself the controller, such as the management of clinic accounts, invoicing, security of the platform and Processor's own website. Processor's privacy statement applies to that processing.

1.4 This agreement applies for as long as Processor processes personal data for Controller and forms part of the arrangements for the use of the Service.

2. Nature, purpose and data

2.1 The purposes, categories of data subjects and categories of personal data are set out in Annex 1.

2.2 Controller does not record special categories of personal data within the meaning of article 9 GDPR in the Service, in particular no data concerning health (such as conditions, allergies, medication or medical history), and does not ask data subjects to provide such data through the Service, including the notes field of an appointment, the internal notes, the web chat and reviews. Such data belongs in Controller's own (medical) records.

2.3 The name of a chosen treatment may in certain cases indirectly reveal something about a data subject's health. Processor uses it solely for scheduling and managing the appointment and does not include it in data sent to advertising platforms, including via web addresses or page titles. Controller ensures that a valid legal basis exists for this processing.

2.4 Processor reminds data subjects not to share medical data (at the notes field, in the first reply of the web chat and in the review form), limits the length of free-text fields and does not let the AI booking assistant ask for health data. Medical questions are passed on to Controller. Reviews are checked automatically for possible health data before publication and, where necessary, assessed by an employee of Processor. If Processor nevertheless receives special categories of personal data, Processor does not process them further than necessary to perform the Service, does not share them with advertising platforms, does not publish them and deletes them at Controller's request.

3. Controller's instructions

3.1 Processor processes personal data solely on the basis of written instructions from Controller, including with regard to transfers to countries outside the EEA, unless a legal obligation requires otherwise. In that case Processor informs Controller in advance, unless the law prohibits this.

3.2 This agreement, the general terms and conditions (including the review rules) and the settings Controller chooses in the Service (such as switching on the web chat, reviews or SMS reminders and connecting an advertising account) count as written instructions.

3.3 Processor informs Controller immediately if, in its opinion, an instruction infringes the GDPR or other data protection rules.

4. Ad measurement

4.1 If Controller connects its own advertising account to the Service (such as Google Ads, and when available TikTok or a Meta dataset), it instructs Processor to send booking events to that account on its behalf, solely under the conditions of this article.

4.2 Processor only sends a booking event if the data subject has given prior, free, specific and unambiguous consent for it through a box that is not ticked in advance, in which the platforms to which the data is passed on are named. The presence of an ad click ID or an advertising cookie does not count as consent. Processor records per booking whether and when consent was given and which version of the consent text was shown.

4.3 Per event, Processor only sends: a booking ID, the time, the type of event, the email address and phone number only in hashed form (SHA-256), advertising identifiers (such as gclid, ttclid, fbclid and advertising cookies), and for website bookings the IP address and browser type and the web address without path and parameters. Processor never sends the chosen treatment, notes, name, chat messages or reviews.

4.4 If the data subject withdraws consent, Processor sends no further events about that data subject from that moment. Data sent earlier is the responsibility of Controller and the platform concerned.

4.5 Advertising platforms are not sub-processors of Processor for this transmission. They receive the data on the basis of the agreements Controller has concluded with them itself (such as the Google Ads Data Processing Terms). Controller is responsible for having accepted these agreements and for its own privacy statement mentioning this processing.

4.6 On the booking page, Processor loads Controller's advertising cookies or pixels only after consent for marketing cookies, with automatic data collection switched off.

5. Confidentiality and security

5.1 Processor ensures that persons with access to the personal data are bound by confidentiality.

5.2 Processor takes appropriate technical and organisational measures as referred to in article 32 GDPR. Annex 3 describes the measures.

6. Sub-processors

6.1 Controller gives general written authorisation for the use of the sub-processors in Annex 2.

6.2 Processor informs Controller by email at least 14 days in advance of a new or replacement sub-processor. Controller may object on reasonable grounds within that period. If the parties cannot reach agreement, Controller may terminate the agreement free of charge.

6.3 Processor imposes on sub-processors obligations at least equivalent to those in this agreement and

remains responsible towards Controller for their fulfilment.

7. Transfers outside the EEA

7.1 Processor stores the data of the Service in the EEA. Transfers outside the EEA only take place to the sub-processors in Annex 2 and only with appropriate safeguards, such as an adequacy decision (including the EU-US Data Privacy Framework) or standard contractual clauses of the European Commission.

8. Data subject rights and assistance

8.1 Processor assists Controller, as far as reasonable, in responding to requests from data subjects (such as access, rectification, erasure and withdrawal of consent). If Processor receives such a request directly, it forwards it within 5 working days.

8.2 Processor assists Controller, as far as reasonable, with the obligations under articles 32 to 36 GDPR, including a data protection impact assessment (DPIA), by providing the necessary information about the Service.

9. Data breaches

9.1 Processor informs Controller without undue delay, and no later than 24 hours after discovery, of a personal data breach.

9.2 Processor provides, as far as known: the nature of the breach, the categories and estimated number of data subjects and records, the likely consequences, the measures taken and proposed, and a contact person. Controller decides on notifying the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) and data subjects.

10. Audit

10.1 On request, Processor makes available the information needed to demonstrate compliance with this agreement. An audit by an independent expert bound by confidentiality is possible after reasonable notice, at most once a year, at Controller's expense.

11. Retention and deletion

11.1 Processor keeps personal data no longer than necessary for the Service, according to the periods in Annex 1, unless Controller sets a shorter period.

11.2 After the Service ends, Processor deletes the personal data within 30 days, or returns it in a common format on request beforehand, unless a statutory retention obligation applies. Backups are overwritten within the usual rotation (at most 30 days after that).

12. Liability

12.1 The parties' liability under this agreement follows the liability arrangements in Processor's general terms and conditions. Each party is responsible towards data subjects and supervisory authorities in accordance with articles 82 and 83 GDPR.

12.2 Controller indemnifies Processor against third-party claims resulting from unlawful instructions of Controller, the absence of a legal basis it was required to have, or the recording of special categories of personal data in breach of article 2.2.

13. Final provisions

13.1 This agreement is governed by Dutch law. Disputes are submitted to the competent court in Amsterdam.

13.2 Processor may change this agreement. A new version is presented for acceptance; until it is accepted, the previous version continues to apply.

13.3 This agreement is accepted electronically. Processor records the name and role of the signatory, the business, the KvK number, the version, the date and time and the IP address of the acceptance.

Annex 1: Processing

Scheduling and managing appointments (calendar), confirmations, reminders by email and SMS

Data subjects: Controller's clients

Personal data: Name, email, phone, language, treatment, date/time, staff member, notes (max. 300 characters), internal notes, status (such as completed or no-show), privacy and marketing choice

Retention period (default): As long as the clinic uses the Service; past and cancelled appointments no later than 24 months after the appointment date

AI booking assistant (web chat) on the booking page, a chat page or the clinic's website

Data subjects: Clients and potential clients

Personal data: Chat messages, name and contact details provided, chosen appointment, ad referral of the page; hashed IP address to prevent abuse

Retention period (default): Conversations 12 months after the last message; hashed IP address at most 7 days

Reviews (if the clinic switches them on): invitation after a completed appointment, posting, checking and showing

Data subjects: Clients with a completed appointment

Personal data: Email address (for the invitation), rating, review text, display name (first name + initial), date, the clinic's reply, reports

Retention period (default): Review text 24 months after publication; rating, date and display name as long as the clinic uses the Service

Notifications to the clinic (email)

Data subjects: Clients; clinic staff

Personal data: Appointment details; name and contact details of staff

Retention period (default): As appointments

Staff and availability

Data subjects: Clinic staff

Personal data: Name, role, working hours, services

Retention period (default): As long as the clinic uses the Service

Ad measurement (article 4)

Data subjects: Clients who gave consent

Personal data: Booking ID, hashed email address and phone number, click IDs, IP address, browser, time

Retention period (default): Sending log: 90 days

Campaign management and cost reporting

Data subjects: n/a

Personal data: Aggregated advertising costs and results, no personal data of clients

Retention period (default): As long as the clinic uses the Service

Annex 2: Sub-processors

Supabase Inc.

Purpose: Database, authentication, storage
Data location: EU (Ireland)
Safeguard for transfers: Standard contractual clauses for any access from the US

Vercel Inc.

Purpose: Hosting of the application
Data location: US (processing), storage in the database in the EU
Safeguard for transfers: EU-US Data Privacy Framework / standard contractual clauses

Resend Inc.

Purpose: Sending email
Data location: US
Safeguard for transfers: Standard contractual clauses

CM.com Netherlands B.V.

Purpose: Sending SMS reminders (if the clinic switches this on)
Data location: NL/EU
Safeguard for transfers: n/a

Anthropic PBC

Purpose: AI booking assistant (web chat) and automatic checking of reviews
Data location: US
Safeguard for transfers: EU-US Data Privacy Framework / standard contractual clauses

Cloudflare Inc.

Purpose: Bot protection (Turnstile) for the web chat
Data location: EU/US
Safeguard for transfers: EU-US Data Privacy Framework / standard contractual clauses

TransIP B.V.

Purpose: Boekenbloom's domain and email
Data location: NL
Safeguard for transfers: n/a

Advertising platforms are not sub-processors: see article 4.5.

Annex 3: Security measures

- Encryption of data in transit (TLS) and at rest.
- Access restriction per clinic at database level (row level security); clinic staff only see data of that clinic.
- Boekenbloom administrator access only with personal accounts and two-step verification (TOTP); administrator actions are logged.
- Secret keys (such as advertising tokens) are stored encrypted and can no longer be read in the dashboard after entry.
- Pseudonymisation (SHA-256) of email address and phone number before sending to advertising platforms; IP addresses for abuse prevention only hashed.
- Bot protection and limits per session and per clinic on registration, login and the web chat.
- Data minimisation: limited free-text fields, warning against medical data, no treatment in advertising data, checking of reviews before publication.

- Automatic deletion according to the retention periods in Annex 1.
- Backups according to the database provider's facilities.
- Policy for reporting and handling security incidents within 24 hours.