

Beveiliging bij PraktijkBaken

Openbaar overzicht van onze beveiligingsmaatregelen

PraktijkBaken is software voor zorg- en welzijnspraktijken: agenda, cliëntdossiers, facturen en communicatie met cliënten. Daarin staan gegevens die vertrouwelijk zijn, waaronder gezondheidsgegevens. Dit overzicht beschrijft hoe we die gegevens beschermen.

Het is geschreven voor praktijkhouders, voor organisaties die met ons samenwerken en voor auditors. Het beschrijft **wat** we doen, niet de technische details van **hoe**: die houden we bewust voor ons, omdat ze aanvallers kunnen helpen. Auditors kunnen een uitgebreider dossier opvragen (zie het laatste hoofdstuk).

1. Onze uitgangspunten

- **Privacy is de standaard.** We verwerken alleen de gegevens die nodig zijn voor de dienst, en niets daarbuiten.
- **Alles blijft in Europa.** Opslag, back-ups en alle sub-verwerkers bevinden zich in de Europese Unie of de Europese Economische Ruimte.
- **Elke praktijk staat op zichzelf.** Gegevens van de ene praktijk kunnen nooit bij een andere terechtkomen.
- **Beveiliging is nooit af.** We controleren, testen en verbeteren doorlopend.

2. Rollen en afspraken

- De **praktijk** is eigenaar van de gegevens van haar cliënten (verwerkingsverantwoordelijke in de zin van de AVG).
- **PraktijkBaken** verwerkt die gegevens uitsluitend in opdracht van de praktijk (verwerker).
- De afspraken staan in onze **verwerkersovereenkomst**. Daarin staat ook de volledige lijst van sub-verwerkers, met hun rol en vestigingsland.

3. Hosting en infrastructuur

- De dienst draait in **datacentra in Duitsland** van een Europese hostingpartij met een ISO 27001-certificering.
- De servers zijn afgeschermd met een netwerkfirewall; alleen de noodzakelijke diensten zijn van buitenaf bereikbaar. De hostingpartij biedt standaard bescherming tegen overbelastingsaanvallen (DDoS).
- Technisch beheer is alleen mogelijk met persoonlijke cryptografische sleutels. Inloggen met alleen een wachtwoord is voor beheer uitgeschakeld.
- Beveiligingsupdates van het besturingssysteem worden automatisch geïnstalleerd.

4. Scheiding tussen praktijken

Elke praktijk heeft een **eigen, afgeschermd omgeving**: een eigen database, eigen bestanden en een eigen systeemaccount waaronder haar software draait. Een fout of misbruik binnen de ene omgeving kan de andere niet bereiken. Binnen de software controleert elke opvraging van een dossier bovendien of het dossier bij de betreffende praktijk hoort.

5. Toegang en inloggen

- **Medewerkers van een praktijk loggen altijd in met hun wachtwoord én een eenmalige inlogcode.** Een gestolen wachtwoord alleen is dus niet genoeg.
- Wachtwoorden worden nooit leesbaar opgeslagen, maar met een modern hash-algoritme dat speciaal voor wachtwoorden is ontworpen.
- Na herhaalde mislukte inlogpogingen wordt het betreffende adres geblokkeerd, voor alle praktijken tegelijk.
- Sessies verlopen automatisch na een periode zonder activiteit.
- Binnen een praktijk bepalen rollen wie wat mag zien. Een behandelaar ziet alleen de cliënten waarvoor hij of zij toegang heeft. Een externe boekhouder krijgt alleen-lezen toegang tot de financiële cijfers, zonder cliëntdossiers.

6. Versleuteling

- Alle verbindingen zijn **versleuteld** (HTTPS met actuele TLS-certificaten). Onversleuteld contact is niet mogelijk.
- Bijzonder gevoelige gegevens, zoals het **burgerservicenummer** en **berichten**, worden daarnaast afzonderlijk versleuteld opgeslagen.
- **Back-ups** worden versleuteld voordat ze de server verlaten. De externe opslagdienst kan de inhoud dus niet lezen.

7. Vastleggen wie wat doet

- Elke praktijk heeft een **toegangslogboek**: wie heeft wanneer welk dossier ingezien of gewijzigd. De praktijk kan dat zelf raadplegen.
- Logboeken bevatten zelf geen medische inhoud, alleen verwijzingen.

8. Bewaking

De dienst wordt **dag en nacht automatisch bewaakt**: bereikbaarheid van elke praktijk, back-ups, certificaten, belasting en verdacht verkeer. Bij afwijkingen gaat er direct een waarschuwing uit.

9. Back-ups en continuïteit

- Er wordt **dagelijks** een volledige back-up gemaakt van elke praktijk, op **meerdere, van elkaar onafhankelijke locaties** binnen Europa.
- Minstens één van de back-uplocaties staat buiten bereik van de server zelf. Een aanvaller die de server zou binnendringen, kan dus niet alle back-ups wissen.
- Het terugzetten van back-ups wordt **automatisch en regelmatig getest**. Een back-up die niet terug te zetten is, is geen back-up.
- Voor verschillende soorten verstoringen ligt een **uitgewerkt noodplan** klaar, dat periodiek wordt beoefend.

10. Veilige ontwikkeling en onderhoud

- Elke wijziging wordt vooraf **automatisch getest** en eerst op een testomgeving uitgerold, voordat hij bij praktijken terechtkomt.
- De software wordt periodiek onderworpen aan een **beveiligingsaudit**. Bevindingen worden opgelost in volgorde van ernst.
- Beveiligingsproblemen die we zelf of via een melding ontdekken, krijgen voorrang boven alle andere werkzaamheden.

11. Leveranciers

- We werken uitsluitend met leveranciers **binnen de EU of de EER**.
- Met elke leverancier die persoonsgegevens verwerkt, is een verwerkersovereenkomst gesloten.
- Waar het kan, krijgt een leverancier alleen versleutelde, voor hem onleesbare gegevens.

12. AI-functies

- AI-functies (zoals hulp bij het schrijven van notities) zijn **optioneel** en per praktijk uit te schakelen.
- Ze worden verwerkt door **Europese leveranciers**, binnen de EU.
- Bij de leveranciers is ingesteld dat ingevoerde gegevens **niet** worden gebruikt om AI-modellen te trainen.
- De ingebouwde helpdeskassistent heeft **geen toegang** tot praktijkgegevens of dossiers.

13. Incidenten en datalekken

- Voor incidenten en datalekken is een **vaste werkwijze** vastgelegd: indammen, onderzoeken, informeren en herstellen, zonder sporen te wissen.
- Betrokken praktijken worden **zonder onredelijke vertraging** geïnformeerd. Onze streeftermijn is **binnen 24 uur** na ontdekking, zodat de praktijk ruim binnen de wettelijke 72 uur kan melden bij de Autoriteit Persoonsgegevens.
- Elk datalek wordt vastgelegd in een register, ook als melden niet nodig is.

14. Wet- en regelgeving en normen

- **AVG:** PraktijkBaken is ingericht op de eisen voor verwerkers, in het bijzonder de beveiligingsplicht (artikel 32) en de meldplicht bij datalekken (artikel 33).
- **Cyberbeveiligingswet (NIS2):** PraktijkBaken valt buiten de reikwijdte van deze wet, maar volgt de maatregelen daaruit waar ze passen: risicobeheer, incidentafhandeling, continuïteit, beveiliging van de leveringsketen, veilige ontwikkeling, versleuteling, toegangsbeheer en meerfactorauthenticatie.
- **NEN 7510 en ISO 27001** gebruiken we als leidraad. PraktijkBaken is daarvoor **niet gecertificeerd** en claimt dat ook niet.

15. Een kwetsbaarheid melden

Vermoedt u een beveiligingsprobleem in PraktijkBaken? Meld het ons via **contact@praktijkbaken.nl**. Vermeld wat u heeft gevonden en hoe we het kunnen nagaan. We reageren snel, behandelen uw melding vertrouwelijk en zullen geen juridische stappen nemen tegen wie te goeder trouw een kwetsbaarheid meldt en die niet misbruikt. Gebruik bij onderzoek geen gegevens van anderen en verstoor de dienst niet.

16. Meer informatie en audits

- Onze openbare pagina **praktijkbaken.nl/gegevensbeveiliging** en de **verwerkersovereenkomst** geven aanvullende informatie.
- **Auditors en organisaties** die een diepgaandere beoordeling moeten doen, kunnen ons **Beveiligingsdossier voor audits** opvragen via **contact@praktijkbaken.nl**. Dat dossier beschrijft onze maatregelen per normonderdeel en wordt verstrekt onder geheimhouding.

PraktijkBaken, contact@praktijkbaken.nl. Dit overzicht wordt minimaal jaarlijks herzien.