

DPIA / GEB - werkdocument

Gegevensbeschermingseffectbeoordeling voor een coachpraktijk die Bloei gebruikt.

Dit document is een vooringevuld werkdocument, geen afgerond besluit. De coach blijft verantwoordelijk voor haar eigen beoordeling, grondslagen, bewaartermijnen en besluit. Laat de uitkomst bij twijfel toetsen door een privacyjurist of FG.

0. Identificatie

Veld	In te vullen
Praktijk / verantwoordelijke	_____
Opsteller en datum	_____
Betrokken FG/jurist	_____
Versie / evaluatiedatum	_____
Betrokken categorieën cliënten	_____

Waarom deze DPIA?

Bloei kan op stelselmatige basis gezondheidsgegevens, vrije dossierinhoud en gegevens van kwetsbare personen verwerken en gebruikt innovatieve AI-ondersteuning. De combinatie kan een hoog privacyrisico opleveren. Rond deze DPIA daarom af vóór grootschalig gebruik en opnieuw bij een wezenlijke wijziging.

1. Systematische beschrijving

Onderdeel	Vooringevulde beschrijving
Doel	Ondersteunen van cliëntbegeleiding: dossier en documenten ordenen, check-ins verwerken, concepten voorbereiden, afspraken en voortgang bewaken.
Betrokkenen	Cliënten van de coach; mogelijk minderjarigen, mensen met gezondheidsproblemen of werknemers in re-integratie.
Gegevens	Identiteit/contact, begeleidings- en gedragsgegevens, documenten, vrije tekst, audio/transcript, mogelijk gezondheidsgegevens en optionele wearable-data.
Rollen	Coach: verwerkingsverantwoordelijke voor cliëntdossier. DutchDesk Holding B.V./Bloei: verwerker. Leveranciers kunnen subverwerker of zelfstandig verantwoordelijke zijn; Oura valt in de tweede categorie.
Datastroom	Browser/app -> Bloei op TransIP (NL). Voor geselecteerde functies minimale inhoud naar Anthropic, OpenAI, Mistral of Resend. Oura-data blijft buiten AI-prompts.
Bewaring	Coach bepaalt dossiertermijn. Bloei: audio 30 dagen, tijdelijke import 24 uur, intake 90 dagen, actieve verwijdering binnen 30 dagen na geverifieerd verzoek; back-upcyclus 30 dagen.

2. Noodzaak en evenredigheid

Toets	Beoordeling / actie coach
Doelbinding	Leg per module vast waarom de verwerking nodig is. Schakel niet-noodzakelijke modules uit.
Grondslag art. 6	Kies en documenteer per doel. In te vullen: _____
Uitzondering art. 9	Bij gezondheidsgegevens: kies en documenteer toepasselijke uitzondering. In te vullen: _____
Minderjarigen	Bepaal wie mag instemmen, welke informatie kind/ouders krijgen en hoe toestemming/gezag wordt gecontroleerd.
Dataminimalisatie	Gebruik alleen noodzakelijke velden; vermijd BSN, volledige geboortedatum en vrije tekst wanneer een minder gevoelig gegeven volstaat.
Transparantie	Geef cliënt de eigen praktijkverklaring en Bloei-1-pager; benoem AI, leveranciers, bewaartermijn en rechten vóór verwerking.
Juistheid	Cliënt kan invoer controleren; coach verifieert dossierimport, AI-concepten en correcties.
Rechten	Leg eigenaar, identiteitstoets, zoekroute, export- en verwijderoute vast. Reageer in beginsel binnen een maand.
Bewaartermijn	Praktijktermijn per dossiertype: _____

3. Risicoanalyse

Risico	Kans	Impact	Voorgaatregel
Accountmisbruik geeft toegang tot gezondheidsgegevens	M	H	H
Verkeerd document aan verkeerde cliënt gekoppeld	M	H	H
AI-concept bevat een onjuist, stigmatiserend of onveilig advies	M	H	H
Naam of bijzondere gegevens gaan onnodig naar AI-leverancier	M	H	H
Opname zonder geldige toestemming of met omstanders	M	H	H
Gegevens minderjarige zonder juiste vertegenwoordiging	L/M	H	H
Verwijderverzoek laat kopie of bestand achter	M	H	H
Doorgifte buiten EER zonder passende waarborg	L/M	H	H
Leverancier of hostingomgeving krijgt een datalek	L/M	H	H
Coach vertrouwt te veel op automatisch signaal	M	M/H	H

Schaal: L = laag, M = midden, H = hoog. Pas kans en impact aan de eigen praktijk, omvang en cliëntgroep aan.

4. Maatregelen en restrisico

Risico	Bloei-maatregel	Coach-maatregel	Restrisico
Onbevoegde toegang	TLS, SQLCipher, praktijkscheiding, sessiebeveiliging, verplichte 2FA en inlogrem	Uniek wachtwoord; apparaatbeleid; toegang periodiek controleren	M
Verkeerde cliënt	Import toont voorstel, bron en conflict vóór opslag	Identiteit op twee kenmerken controleren	L/M
Onjuist AI-concept	Geen automatische verzending; tweede controlelaag; bron en concept onderscheiden	Inhoudelijk nalezen; crisis- en verwijsprotocol volgen	M
Onnodige AI-data	Pseudonimisatie en dataminimalisatie waar mogelijk	Geen namen in vrije tekst; opname/document alleen indien noodzakelijk	M
Opname	Zichtbare toestemmingspoort; audio maximaal 30 dagen	Vooraf informeren; toestemming en aanwezig vastleggen	M
Minderjarigen	Aparte kindmodus en menselijke controle	Gezag/leeftijd controleren; kindvriendelijk informeren	M
Bewaring/verwijdering	Concrete termijnen, export en verwijderproces; back-upcyclus	Eigen dossiertermijn; periodieke opschoning; verzoeklog	L/M
Internationale doorgifte	EU-SCC's en aanvullende maatregelen	Alleen noodzakelijke modules gebruiken; documentatie bewaren	M
Datalek	Monitoring, back-up, incidentprocedure en snelle melding	Eigen incidentcontact en 72-uursproces oefenen	M

5. Raadpleging en besluit

Vraag	Besluit / onderbouwing
Zijn cliënten of vertegenwoordigers geraadpleegd?	_____
Is een FG/privacyjurist geraadpleegd?	_____
Blijft na maatregelen een hoog restrisico bestaan?	Ja / nee. Toelichting: _____
Is voorafgaande raadpleging van de AP nodig?	Ja / nee. Toelichting: _____
Besluit	Starten / aanpassen / niet starten
Voorwaarden en actiehouders	_____
Naam, functie, datum, handtekening	_____
Eerstvolgende evaluatie	_____

Minimale bewijsmap

- Deze ingevulde DPIA en de datum van besluit/evaluatie.
- Verwerkersovereenkomst v2.0 en actuele subverwerkerslijst.
- Eigen privacyverklaring en cliëntinformatie.
- Grondslagen- en bewaartermijnenoverzicht per module.
- Procedure voor privacyverzoeken en datalekregister.
- Bewijs van periodieke toegangs-, verwijder- en hersteltests.