

1. Doel en toepassingsgebied

Deze richtlijn beschrijft de beginselen voor het veilig, rechtmatig en zorgvuldig omgaan met persoonsgegevens en communicatie binnen huidtherapiepraktijken aangesloten bij BVHN. De richtlijn richt zich op alle vormen van verwerking en uitwisseling van persoonsgegevens en is van toepassing op alle medewerkers, stagiaires en externe verwerkers die betrokken zijn bij de zorgverlening.

2. Juridisch kader

De verwerking en communicatie van persoonsgegevens binnen de huidtherapie valt onder:

- AVG (EU 2016/679)
- Uitvoeringswet AVG (UAVG)
- WGBO – bepalingen voor het medisch dossier en informatieverstrekking
- Wabvpz – elektronische gegevensverwerking en logging
- Wkkgz – veilig incidenten melden en openheid
- NEN7510 – normen voor informatiebeveiliging in de zorg

Deze wet- en regelgeving is leidend voor alle bepalingen in deze richtlijn.

3. Beginselen van gegevensverwerking

Persoonsgegevens worden verwerkt volgens de basisprincipes van de AVG:

1. Rechtmatigheid, behoorlijkheid en transparantie
2. Doelbinding
3. Dataminimalisatie
4. Juistheid
5. Opslagbeperking (met inachtneming van WGBO-bewaarplichten)
6. Integriteit en vertrouwelijkheid
7. Accountability (verantwoordingsplicht)

Bijzondere persoonsgegevens (waaronder medische gegevens) worden uitsluitend verwerkt wanneer een rechtmatige verwerkingsgrondslag aanwezig is.

4. Verwerkingsgrondslagen

Verwerking van persoonsgegevens binnen de huidtherapie vindt in hoofdzaak plaats op basis van:

- uitvoering van de **behandelingsovereenkomst** (WGBO);
 - **wettelijke verplichtingen** die volgen uit o.a. WGBO, Wkkgz;
 - **toestemming** van de betrokkene wanneer vereist;
 - **gerechtvaardigd belang** binnen de grenzen van professionele zorgkwaliteit;
 - **vitale belangen** in uitzonderlijke situaties.
-

5. Organisatorische verantwoordelijkheden

Huidtherapiepraktijken moeten zorgen voor:

- een interne verdeling van verantwoordelijkheden en bevoegdheden;
 - schriftelijk beleid voor gegevensbescherming en communicatie;
 - een actuele autorisatiematrix;
 - procedures voor toegang, wijziging en verwijdering van gegevens;
 - naleving van geheimhoudingsverplichtingen door medewerkers.
-

6. Technische en organisatorische beveiligingsmaatregelen

Praktijken nemen passende beveiligingsmaatregelen in lijn met AVG art. 32 en NEN7510, waaronder:

- toegangsbeveiliging met meerfactorauthenticatie waar passend;
- logging en controle op toegang tot elektronische dossiers (Wabvpz);
- beveiligde opslag en bescherming tegen ongeautoriseerde toegang;
- veilige configuratie van digitale systemen;
- beleid voor het gebruik van apparaten;
- processen die dataminimalisatie bevorderen;

- periodieke toetsing van beveiligingsmaatregelen.
-

7. Communicatie van persoonsgegevens

De praktijk waarborgt dat communicatie over persoonsgegevens:

- uitsluitend plaatsvindt via **passend beveiligde** communicatiemiddelen;
- voldoet aan de eisen van vertrouwelijkheid, integriteit en controleerbaarheid;
- voldoet aan de beveiligingsregels van AVG, Wabvpz en NEN7510;
- beperkt blijft tot informatie die noodzakelijk is voor zorgverlening of wettelijke verplichtingen;
- alleen toegankelijk is voor bevoegde medewerkers.

De praktijk differentieert tussen communicatie die **geen bijzondere persoonsgegevens** bevat en communicatie die **medische of andere bijzondere gegevens** omvat, waarbij voor de laatste categorie strengere beveiliging geldt.

8. Foto's en beeldmateriaal

Verwerking van foto's of andere beelden van cliënten wordt gezien als verwerking van bijzondere persoonsgegevens.

De praktijk waarborgt dat:

- verwerking alleen plaatsvindt met een geldige grondslag (veelal toestemming of uitvoering van de behandelingsovereenkomst);
 - opslag en uitwisseling beveiligd en controleerbaar plaatsvinden;
 - alleen bevoegde medewerkers toegang hebben tot het materiaal;
 - gebruik en bewaartermijnen aansluiten bij dossier- en privacywetgeving.
-

9. Rechten van cliënten

De praktijk faciliteert de uitoefening van alle rechten van betrokkenen zoals gedefinieerd in de AVG, waaronder:

- recht op inzage;
- recht op rectificatie;
- recht op aanvulling;

- recht op gegevensbeperking;
- recht op dataportabiliteit;
- recht op vernietiging voor zover dit volgens WGBO mogelijk is.

Verzoeken worden binnen wettelijke termijnen afgehandeld.

10. Externe verwerkers

Wanneer persoonsgegevens worden verwerkt door externe partijen, zorgt de praktijk voor:

- een **verwerkersovereenkomst** (AVG art. 28);
 - toetsing aan beveiligingsnormen;
 - documentatie van de verwerkingsactiviteiten;
 - toezicht op naleving door de verwerker.
-

11. Datalekken

De praktijk beschikt over een procedure voor datalekken die voldoet aan:

- verplichtingen van AVG art. 33 en 34;
 - registratie van alle datalekken;
 - beoordeling van risico's voor betrokkenen;
 - melding aan de Autoriteit Persoonsgegevens wanneer vereist;
 - informeren van cliënten indien hun rechten of vrijheden mogelijk worden geschaad.
-

12. Documentatie- en bewaarplichten

De praktijk voldoet aan:

- de bewaartermijn van **20 jaar** (WGBO) voor medische dossiers;
- aanvullende wettelijke bewaartermijnen indien relevanter;
- opslagbeperking voor niet-medische persoonsgegevens conform AVG;
- beschikbaarheid en actualiteit van alle verplichte documenten, waaronder:
 - verwerkingsregister;

- privacybeleid;
 - datalekregister;
 - autorisatiematrix;
 - verwerkersovereenkomsten;
 - beleid veilige communicatie.
-

13. Inwerkingtreding

Deze richtlijn treedt in werking op **1 januari 2026** en maakt integraal deel uit van het BVHN Kwaliteitskader.