

Privacy beleid

1. Inleiding

In lijn met de Algemene Verordening Gegevensbescherming (AVG), de Europese Gezondheidsgegevensruimte (EHDS), de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO), de Wet toetreding zorgaanbieders (Wtza), de Wet gegevensverwerking door samenwerkingsverbanden (Wgs) en overige relevante wetgeving hanteert Thuiszorg Zorg voor Later B.V. een privacyreglement.

Dit reglement heeft als doel de bescherming van persoonsgegevens en de privacy van cliënten en medewerkers te waarborgen. Thuiszorg Zorg voor Later B.V. hecht grote waarde aan privacy en verplicht alle medewerkers dit reglement na te leven. Privacy gaat niet alleen over het beschermen van persoonsgegevens, maar ook over de bescherming van het lichaam, de woon- en leefomgeving van de cliënt en het vertrouwelijk omgaan met zorgrapportages.

Dit reglement is opgesteld volgens de richtlijnen van:

- De Algemene Verordening Gegevensbescherming (AVG)
- De Europese Gezondheidsgegevensruimte (EHDS) Verordening
- De Wet toetreding zorgaanbieders (Wtza)
- De Wet op de Geneeskundige Behandelingsovereenkomst (WGBO)
- De geheimhoudingsplicht van zorgverleners (WGBO artikel 7:457) en aanvullend de toepasselijke CAO
- De Wet gegevensverwerking door samenwerkingsverbanden (Wgs)

2. Verantwoordelijkheden

De verantwoordelijkheid voor het privacy- en informatiebeveiligingsbeleid is als volgt verdeeld:

- Bestuur en management zijn verantwoordelijk voor het vaststellen, actualiseren en bewaken van dit beleid en het privacyreglement.
- Leidinggevenden zorgen voor implementatie en naleving van het beleid binnen hun teams.
- Functionaris Gegevensbescherming (FG):
 - Thuiszorg Zorg voor Later B.V. heeft een FG aangewezen conform artikel 37 AVG.
 - De FG houdt toezicht op de verwerking van persoonsgegevens, voert audits uit, beoordeelt Data Protection Impact Assessments (DPIA's) en adviseert het management over privacyvraagstukken.
- Alle medewerkers zijn verantwoordelijk voor het naleven van het privacy beleid en handelen volgens de richtlijnen voor gegevensbescherming en informatiebeveiliging.

PRIVACY VAN CLIËNTEN

3. Informatie aan de cliënt

Bij het eerste zorgcontact wordt de cliënt mondeling en/of schriftelijk geïnformeerd over hoe Thuiszorg Zorg voor Later B.V. omgaat met zijn/haar persoonsgegevens. De cliënt krijgt informatie over waar dit privacyreglement te vinden is (website van Thuiszorg Zorg voor Later B.V.) en kan dit op ieder moment raadplegen.

In begrijpelijke taal wordt toegelicht:

- welke categorieën persoonsgegevens worden verzameld;
- voor welke doeleinden deze gegevens worden gebruikt;

- op welke rechtsgrond de verwerking berust (bijvoorbeeld uitvoering behandelovereenkomst op grond van de WGBO, wettelijke verplichting, of gerechtvaardigd belang);
- hoe lang de gegevens worden bewaard of welke criteria voor de bewaartermijnen worden gehanteerd;
- met welke partijen de gegevens eventueel worden gedeeld (bijvoorbeeld andere zorgverleners, zorgverzekeraars, ICT-dienstverleners);
- welke rechten de cliënt heeft (zoals inzage, correctie, verwijdering, beperking, bezwaar en dataportabiliteit);
- hoe een klacht kan worden ingediend bij Thuiszorg Zorg voor Later B.V. en bij de Autoriteit Persoonsgegevens;
- waar het volledige privacyreglement online beschikbaar is.

Indien gebruik wordt gemaakt van digitale portalen of elektronische uitwisseling van gegevens, wordt de cliënt hierover eveneens geïnformeerd.

4. Doeleinden van de verwerking van cliëntgegevens

De persoonsgegevens van cliënten worden verwerkt voor de volgende doeleinden:

- Het bieden van zorg, hulp en diensten die door Thuiszorg Zorg voor Later B.V. worden geleverd (uitvoering behandelovereenkomst op grond van de WGBO);
- Het vastleggen en beschikbaar stellen van gegevens voor doelmatig beleid en beheer van de organisatie;
- Het uitvoeren van kwaliteitscontroles om de zorgverlening te verbeteren;
- Het financieel afhandelen van de geleverde zorg met de cliënt of diens zorgverzekeraar;
- Het verantwoorden van de organisatie aan zorgverzekeraars en overheidsinstanties, conform de wettelijke verplichtingen;
- Het evalueren en onderzoeken van de zorg- en dienstverlening, waar mogelijk in gepseudonimiseerde of geanonimiseerde vorm.

Thuiszorg Zorg voor Later B.V. zal geen persoonsgegevens van cliënten verwerken voor andere doeleinden dan hierboven vermeld, tenzij daarvoor een nieuwe rechtsgrond bestaat en de cliënt hierover tijdig en duidelijk is geïnformeerd.

5. Bewaartermijnen voor cliëntgegevens

5.1 Medische (zorg)dossiers cliënten

Voor medische dossiers van cliënten geldt de wettelijke bewaartermijn zoals bepaald in de WGBO:

- Medische (zorg)dossiers worden 20 jaar bewaard, gerekend vanaf het moment van de laatste wijziging in het dossier, tenzij uit de zorg van een goed hulpverlener voortvloeit dat gegevens langer bewaard moeten blijven (bijvoorbeeld in verband met chronische aandoeningen of mogelijke claims).

Indien specifieke wetgeving (bijvoorbeeld jeugdwetgeving of bijzondere sectorale regels) een langere of kortere bewaartermijn voorschrijft, wordt die termijn toegepast. Deze uitzonderingen worden in het interne archiverings- en bewaarbeleid nader gespecificeerd.

5.2 Financiële gegevens cliënten

- Facturen, declaraties en andere financiële bescheiden met persoonsgegevens van cliënten worden in principe 7 jaar bewaard, conform fiscale wetgeving.

5.3 Gegevens over klachten en incidenten (cliënten)

- Gegevens met betrekking tot klachten en incidenten worden in principe 5 jaar na afhandeling bewaard, tenzij een langere termijn noodzakelijk is in verband met (mogelijke) juridische procedures of kwaliteitsevaluaties.

6. Rechten van cliënten

Cliënten hebben op grond van de AVG en de WGBO de volgende rechten:

- Recht op inzage in hun persoons- en medische gegevens;
- Recht op afschrift van het medisch dossier;
- Recht op correctie/aanvulling van onjuiste of onvolledige gegevens;
- Recht op verwijdering van gegevens, voor zover dit niet in strijd is met de wettelijke bewaartermijnen;
- Recht op beperking van de verwerking;
- Recht op overdraagbaarheid (dataportabiliteit) van hun persoonsgegevens, voor zover technisch mogelijk;
- Recht op bezwaar tegen bepaalde verwerkingen;
- Recht om een eerder gegeven toestemming in te trekken, zonder terugwerkende kracht.

Verzoeken worden in principe binnen 30 dagen afgehandeld. Indien meer tijd nodig is, wordt de betrokkene binnen 30 dagen geïnformeerd over de reden van uitstel en de verwachte termijn.

Cliënten hebben daarnaast het recht om inzicht te krijgen in wie hun elektronische dossier heeft geraadpleegd en wanneer, conform de Wabvpz/WGBO-bepalingen over logging.

7. Gegevensdeling met derden (cliënten)

Persoonsgegevens van cliënten worden uitsluitend gedeeld met derden indien:

- dit noodzakelijk is voor de uitvoering van de behandelovereenkomst (bijvoorbeeld met de huisarts, specialist of andere betrokken zorgverleners),
- dit noodzakelijk is om te voldoen aan een wettelijke verplichting (bijvoorbeeld richting zorgverzekeraar of toezichthouder), of
- de cliënt daarvoor uitdrukkelijk en specifiek toestemming heeft gegeven.

Met alle verwerkers (zoals ICT-dienstverleners, ECD-leveranciers en AI-dienstverleners) worden verwerkersovereenkomsten gesloten, waarin onder andere:

- de doeleinden en middelen van de verwerking zijn vastgelegd,
- passende technische en organisatorische maatregelen zijn afgesproken,
- is vastgelegd dat persoonsgegevens niet voor eigen (trainings)doeleinden van de verwerker worden gebruikt, tenzij dit uitdrukkelijk en rechtsgeldig is toegestaan.

Uitwisseling van gegevens met derden vindt altijd plaats met inachtneming van het beroepsgeheim van zorgverleners (WGBO artikel 7:457).

8. Europese Gezondheidsgegevensruimte (EHDS)

Thuiszorg Zorg voor Later B.V. houdt rekening met de regels van de Europese Gezondheidsgegevensruimte (EHDS). Dit betekent onder meer dat cliënten:

- recht hebben op tijdige en kosteloze elektronische inzage in hun gezondheidsgegevens, voor zover deze elektronisch beschikbaar zijn;

- hun gezondheidsgegevens eenvoudig kunnen laten overdragen aan andere zorgverleners, ook grensoverschrijdend binnen de Europese Unie, voor zover dit technisch en wettelijk mogelijk is;
- zeggenschap hebben over wie hun gezondheidsgegevens mag inzien en onder welke voorwaarden;
- erop mogen vertrouwen dat secundair gebruik van hun gezondheidsgegevens (bijvoorbeeld voor onderzoek of statistiek) alleen plaatsvindt indien dat is toegestaan op grond van wet- en regelgeving en, waar nodig, met hun toestemming of met inachtneming van een opt-out-regeling.

Nadere uitwerking van EHDS-verplichtingen en -rechten volgt de nationale implementatie in Nederland (inclusief de rol van de Health Data Access Body (HDAB)).

PRIVACY VAN MEDEWERKERS

9. Informatie aan de medewerker

Nieuwe medewerkers worden bij indiensttreding geïnformeerd over dit privacyreglement en over de wijze waarop Thuiszorg Zorg voor Later B.V. met hun persoonsgegevens omgaat. Dit privacyreglement is beschikbaar via het kwaliteitshandboek en/of intranet.

10. Doeleinden van de verwerking van medewerker gegevens

Persoonsgegevens van medewerkers worden verwerkt voor:

- het uitvoeren van het personeelsbeleid;
- het voeren van salaris- en verzuimadministratie;
- het voldoen aan fiscale en arbeidsrechtelijke verplichtingen;
- het uitvoeren van kwaliteits- en functioneringsgesprekken;
- opleidings- en scholingsdoeleinden;
- het waarborgen van veiligheid en integriteit binnen de organisatie.

11. Bewaartermijnen voor medewerker gegevens

Voor persoonsgegevens van (ex-)medewerkers gelden in principe kortere bewaartermijnen dan voor medische dossiers van cliënten. Thuiszorg Zorg voor Later B.V. hanteert hierbij de volgende uitgangspunten:

- Personeelsdossiers worden in beginsel maximaal 2 jaar na uitdiensttreding bewaard, tenzij een langere bewaartermijn noodzakelijk is vanwege wettelijke verplichtingen of lopende (juridische) procedures.
- Gegevens die relevant zijn voor de loonadministratie (bijvoorbeeld salarisgegevens, pensioenafdrachten) worden 7 jaar bewaard, conform fiscale wetgeving.
- Gegevens over (arbeidsrechtelijke) geschillen kunnen langer worden bewaard indien dit nodig is voor de afwikkeling van die geschillen.

Deze termijnen worden nader uitgewerkt in het interne archiverings- en bewaartermijnenbeleid.

12. Geheimhoudingsplicht voor medewerkers

Alle medewerkers zijn op grond van de WGBB (artikel 7:457), de AVG en de toepasselijke CAO gehouden tot geheimhouding van alle persoonsgegevens en medische gegevens die zij in het kader van hun functie verwerken. Deze geheimhoudingsplicht blijft ook na beëindiging van het dienstverband van kracht.

Medewerkers met direct cliëntcontact hebben extra aandacht voor vertrouwelijkheid en informatiebeveiliging. Zij hebben alleen toegang tot persoonsgegevens voor zover dat noodzakelijk is voor hun werkzaamheden ("need to know").

ALGEMENE BEPALINGEN (CLIËNTEN EN MEDEWERKERS)

13. Rechtsgrondslag voor verwerking

Voor elke verwerking van persoonsgegevens is een rechtmatige grondslag vereist.

Thuiszorg Zorg voor Later B.V. verwerkt persoonsgegevens uitsluitend indien één van de volgende grondslagen van toepassing is:

- de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de behandelovereenkomst met de cliënt);
- de verwerking is nodig om te voldoen aan een wettelijke verplichting (bijvoorbeeld op grond van de WGBO, Wlz, Zvw, Wmo, fiscale wetgeving);
- de verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of een andere natuurlijke persoon;
- de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van uitoefening van het openbaar gezag;
- de verwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang van Thuiszorg Zorg voor Later B.V. of van een derde, waarbij de belangen of grondrechten van de betrokkene niet zwaarder wegen;
- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.

Voor de verwerking van gezondheidsgegevens (bijzondere persoonsgegevens) geldt dat deze in de zorgsector doorgaans worden verwerkt op grond van de behandelovereenkomst en de WGBO (en dus niet primair op basis van toestemming). Toestemming wordt alleen gebruikt als grondslag wanneer dat juridisch passend en noodzakelijk is.

14. Beveiliging van persoonsgegevens

Thuiszorg Zorg voor Later B.V. treft passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Hierbij wordt aangesloten bij de normen voor informatiebeveiliging in de zorg, waaronder NEN 7510 en NEN 7512.

14.1 Werkruimtes en apparatuur

- Werkruimtes zijn alleen toegankelijk voor bevoegde personen.
- Apparatuur (computers, laptops, tablets, mobiele telefoons) is beveiligd met sterke wachtwoorden en, waar mogelijk, met Multi-factor authenticatie.
- Apparatuur wordt vergrendeld wanneer deze niet in gebruik is.

14.2 Elektronische communicatie en externe verzending

- Privacygevoelige informatie wordt uitsluitend verzonden via beveiligde elektronische kanalen (bijvoorbeeld beveiligde e-mail, versleutelde verbindingen).
- Bij verzending van papieren documenten met privacygevoelige informatie worden deze in een gesloten envelop met de vermelding "Vertrouwelijk" verzonden.

14.3 Digitale dossiers en logging

- Persoonsgegevens van cliënten en medewerkers worden uitsluitend opgeslagen in beveiligde digitale systemen.
- De systemen maken gebruik van:
 - versleuteling van gevoelige gegevens;
 - sterke authenticatie en rol gebaseerde toegangsrechten;

- automatische logboeken van inzien, muteren en verwijderen van gegevens;
- regelmatige back-ups.

Cliënten hebben het recht om op verzoek een overzicht te verkrijgen van wie hun dossier heeft ingezien en wanneer (logging-inzage).

15. Gebruik van AI-hulpmiddelen

Thuiszorg Zorg voor Later B.V. maakt in beperkte mate gebruik van AI-hulpmiddelen (zoals tekst- en documentassistenten) om medewerkers te ondersteunen bij administratieve en documentatie gerelateerde werkzaamheden.

- AI-hulpmiddelen hebben een puur ondersteunend karakter en nemen nooit zelfstandig beslissingen over de inhoud van zorg of over het al dan niet verlenen, wijzigen of beëindigen van zorg.
- Zuiver geautomatiseerde besluitvorming die rechtsgevolgen heeft of de betrokkene in aanmerkelijke mate treft, is niet toegestaan (conform artikel 22 AVG).
- Medewerkers blijven altijd zelf verantwoordelijk voor de inhoud, juistheid en volledigheid van documenten en zorgplannen. Zij controleren en beoordelen AI-voorstellen voordat deze in een dossier worden opgeslagen.
- Met leveranciers van AI-hulpmiddelen worden verwerkersovereenkomsten gesloten waarin is vastgelegd dat persoonsgegevens niet worden gebruikt voor modeltraining of productverbetering, tenzij dit uitdrukkelijk en rechtsgeldig is toegestaan.

Cliënten kunnen desgewenst aangeven dat hun zorgplan volledig zonder gebruik van AI-hulpmiddelen wordt opgesteld.

16. Data Protection Impact Assessments (DPIA)

Voor verwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen (zoals de invoering van nieuwe ICT-systemen, cloudoplossingen of AI-toepassingen voor gezondheidsgegevens), voert Thuiszorg Zorg voor Later B.V. een Data Protection Impact Assessment (DPIA) uit.

- De DPIA wordt uitgevoerd vóór de start van de betreffende verwerking.
- De FG wordt bij de DPIA betrokken en adviseert over risico's en mitigerende maatregelen.
- De uitkomsten en genomen maatregelen worden gedocumenteerd en periodiek geëvalueerd.

17. Incidenten en datalekken

Onder een datalek wordt verstaan: een inbreuk op de beveiliging die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van, dan wel ongeoorloofde toegang tot, doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Bij (vermoede) datalekken:

- wordt het incident onmiddellijk intern gemeld volgens het interne meldprotocol;
- wordt het incident onderzocht en worden passende maatregelen genomen;
- wordt, indien het datalek waarschijnlijk een risico inhoudt voor de rechten en vrijheden van betrokkenen, dit binnen 72 uur gemeld bij de Autoriteit Persoonsgegevens;
- worden betrokkenen geïnformeerd indien het datalek waarschijnlijk een hoog risico voor hun rechten en vrijheden oplevert, tenzij de wet dit niet vereist of aanvullende maatregelen dit overbodig maken.

Alle datalekken en maatregelen worden vastgelegd in een datalekregister.

18. Verwerking, bewaring en vernietiging van gegevens

- Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of waarvoor zij verder worden verwerkt, met inachtneming van de wettelijke bewaartermijnen.
- Na afloop van de bewaartermijn worden persoonsgegevens op een veilige en verifieerbare wijze vernietigd (digitale gegevens door veilige verwijdering, papieren gegevens door bijvoorbeeld shredding).

Voor cliënten en medewerkers gelden afzonderlijke bewaartermijnen, zoals beschreven in de paragrafen over bewaartermijnen.

19. Doorgifte van gegevens buiten de EER

Indien persoonsgegevens buiten de Europese Economische Ruimte (EER) worden verwerkt, gebeurt dit uitsluitend indien sprake is van passende waarborgen in de zin van de AVG (zoals een adequaatheidsbesluit, Standard Contractuele Clauses of Binding Corporate Rules) en, waar nodig, aanvullende technische en organisatorische maatregelen zoals versleuteling en pseudonimisering.

Met alle partijen die persoonsgegevens buiten de EER verwerken worden verwerkersovereenkomsten gesloten waarin de bescherming van persoonsgegevens contractueel is geborgd.

20. Camera's

Thuiszorg Zorg voor Later B.V. maakt zelf geen gebruik van eigen camera's. Het kantoorgebouw waarin Thuiszorg Zorg voor Later B.V. is gevestigd bevat beveiligingscamera's bij de balie en in- en uitgangen. Deze camera's zijn in beheer van de eigenaar van het pand en vallen buiten de verantwoordelijkheid van Thuiszorg Zorg voor Later B.V.

Voor vragen over deze beveiligingscamera's, inclusief hun werking, doel en bewaartermijn, worden betrokkenen verwezen naar de eigenaar van het pand en diens privacybeleid.

21. Klachten

Indien cliënten of medewerkers een klacht hebben over de verwerking van hun persoonsgegevens, kunnen zij deze melden bij Thuiszorg Zorg voor Later B.V. via de gebruikelijke klachtenprocedure.

Indien een klacht niet naar tevredenheid is afgehandeld, heeft de betrokkene het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

22. Contactgegevens

Thuiszorg Zorg voor Later B.V.

Laan van Bol'es 3A

3122 AE Schiedam

E-mail: info@zorgvoorlater.me

Functionaris Gegevensbescherming (FG):

- Naam: r. de Boer
- E-mail: r.deboer@zorgvoorlater.me

Dit privacyreglement is te allen tijde te raadplegen via het kwaliteitshandboek en op de website van Thuiszorg Zorg voor Later B.V.

23. Disclaimer

Dit privacyreglement is een begrijpelijke samenvatting van de geldende privacywetgeving en is gebaseerd op de AVG, de WGBO, de EHDS-verordening en overige toepasselijke Nederlandse wet- en regelgeving. Indien wet- en regelgeving wijzigt, zal dit reglement worden geactualiseerd.