AVG-beleid

Vitaal Zorggroep

Inhoud

1. Inleiding

Vitaal Zorggroep hecht grote waarde aan de bescherming van persoonsgegevens van iedereen die bij onze organisatie betrokken is: cliënten, medewerkers, vrijwilligers, zzp'ers, stagiairs, mantelzorgers en externe partners. In een tijd waarin digitalisering, samenwerking en datagedreven werken steeds belangrijker worden, is het zorgvuldig en rechtmatig omgaan met persoonsgegevens van essentieel belang – zowel voor het waarborgen van privacyrechten als voor het behouden van vertrouwen.

Met dit AVG-beleid leggen wij vast hoe Vitaal Zorggroep invulling geeft aan de verplichtingen uit de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG) en relevante sectorspecifieke wetgeving zoals de Wet op de geneeskundige behandelingsovereenkomst (WGBO) en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz). Ook sluit dit beleid aan op de normen voor informatiebeveiliging in de zorg, in het bijzonder de NEN7510.

Dit document biedt:

- Een beschrijving van de principes en uitgangspunten van ons privacybeleid;
- Een overzicht van rollen, verantwoordelijkheden en procedures;
- Informatie over hoe wij de rechten van betrokkenen waarborgen;
- Kaders voor veilige en transparante gegevensverwerking binnen al onze zorg- en bedrijfsprocessen;
- Aansluiting op ons bredere stelsel van kwaliteits- en risicomanagement, zoals beschreven in het Jaarplan en -planning Privacy en Informatiebeveiliging 2025–2026.

Dit beleid geldt voor de gehele organisatie: Vitaal Zorggroep B.V. en al haar dochtermaatschappijen waaronder LiefsThuis Ondersteuning, Talenty, BabyCare Kraamzorg, 't Keizertje, en LiefsThuis Zorg. Daarmee is het een integraal kader voor gegevensverwerking in al onze zorg-, ondersteunings- en bedrijfsvoeringsactiviteiten.

Met dit beleid vervangen wij het vorige AVG-beleid 2022–2024. Het huidige beleid is geactualiseerd op basis van gewijzigde wetgeving, technologische ontwikkelingen, nieuwe risicoanalyses (DPIA's), interne audits en geleerde lessen uit de praktijk.

Wil je daarnaast meer weten over wie dit beleid betreft, welke begrippen we gebruiken en welke risico's er zijn? Bekijk dan de bijlagen en verdiepingsinformatie aan het einde van dit document.

2. Doel en reikwijdte

Het beleid is van toepassing op alle verwerkingen van persoonsgegevens binnen Vitaal Zorggroep en haar dochtermaatschappijen. Het biedt kaders voor een privacybewuste cultuur en praktische handvatten voor dagelijkse zorg- en bedrijfsvoering.

Het beleid geldt expliciet voor:

- Vitaal Zorggroep (ondersteunende diensten),
- BabyCare Kraamzorg,
- LiefsThuis Ondersteuning,
- LiefsThuis Zorg,
- Talenty (wonen en dagbesteding),
- 't Keizertje (kinderopvang).

Voor al deze onderdelen gelden dezelfde normen, principes en verantwoordelijkheden op het gebied van privacy en gegevensbescherming, zoals beschreven in dit beleid. Daar waar specifieke verschillen gelden (bijvoorbeeld in type zorg of verwerking), wordt dit nader gespecificeerd in de onderliggende documenten of verwerkingsregisters.

3. Rollen en verantwoordelijkheden

Vitaal Zorggroep kent een duidelijke verdeling van rollen en verantwoordelijkheden op het gebied van privacy en gegevensbescherming. Dit zorgt voor structuur, overzicht en heldere aanspreekpunten binnen de gehele organisatie.

De hoofdtaken en verantwoordelijkheden zijn als volgt:

- Bestuur – eindverantwoordelijk voor het borgen van privacy en informatieveiligheid op strategisch niveau;
- Functionaris Gegevensbescherming (FG) – houdt onafhankelijk toezicht, adviseert en toetst naleving van privacywetgeving;
- Privacy Officer – coördineert de uitvoering van het privacybeleid, voert analyses uit en verzorgt interne rapportages;
- Aandachtsvelders privacy – zorgen voor de lokale inbedding van beleid in de praktijk van de diverse organisatieonderdelen;
- Medewerkers – zijn verantwoordelijk voor zorgvuldige omgang met persoonsgegevens in het dagelijks werk.

Een nadere beschrijving van deze rollen, hun bevoegdheden en onderlinge afstemming is opgenomen in **Bijlage 1 – Rollen en verantwoordelijkheden**.

Privacyteam Vitaal Zorggroep

Het privacyteam van Vitaal Zorggroep is verantwoordelijk voor de praktische uitvoering, bewaking en continue verbetering van het privacybeleid binnen alle organisatieonderdelen. Het team komt minimaal zes keer per jaar bijeen en bestaat uit:

- De Privacy Officer (voorzitter en coördinator);
- Aandachtsvelders privacy vanuit de dochtermaatschappijen;
- Een vertegenwoordiger van het ICT-team (voor technische borging);
- De Functionaris Gegevensbescherming (FG) (externe, onafhankelijke rol);
- Een lid van het bestuur (voor strategische aansluiting).

Het privacyteam bespreekt signalen en risico's, stemt beleidswijzigingen af, evalueert DPIA's en coördineert voorlichtingsactiviteiten. Het team is tevens een klankbord voor de Functionaris Gegevensbescherming.

4. Uitgangspunten privacybeleid

De verwerking van persoonsgegevens binnen Vitaal Zorggroep gebeurt op basis van de volgende fundamentele uitgangspunten uit de AVG:

1. **Rechtmatigheid, transparantie en doelbinding**
    - Persoonsgegevens worden alleen verwerkt op basis van een geldige juridische grondslag.
    - Betrokkenen worden op een begrijpelijke en tijdige manier geïnformeerd over de verwerking van hun gegevens.
    - Gegevens worden uitsluitend verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen.
2. **Dataminimalisatie**
    - Alleen persoonsgegevens die noodzakelijk zijn voor het doel van de verwerking worden verzameld.
    - Overbodige of irrelevante gegevens worden niet verwerkt.
3. **Juistheid, bewaarbeperking en integriteit**
    - Persoonsgegevens zijn juist, volledig en worden zo nodig geactualiseerd.
    - Gegevens worden niet langer bewaard dan noodzakelijk is voor het doel van de verwerking, met inachtneming van wettelijke termijnen.

- Er worden passende technische en organisatorische maatregelen genomen om verlies, misbruik of onbevoegde toegang tot persoonsgegevens te voorkomen.

4. **Verantwoording en accountability**
    - Vitaal Zorggroep kan aantonen dat zij voldoet aan de AVG (verantwoordingsplicht).
    - Dit gebeurt onder andere via een actueel verwerkingsregister, vastgelegde procedures, audits en rapportages.
    - De Functionaris Gegevensbescherming en de Privacy Officer monitoren de naleving van het beleid en adviseren over verbetermaatregelen.

5. Rechten van betrokkenen

Vitaal Zorggroep erkent en faciliteert de volgende privacyrechten van betrokkenen:

1. **Recht op inzage** – het recht om te weten welke gegevens worden verwerkt.
2. **Recht op rectificatie** – het recht om onjuiste gegevens te laten corrigeren.
3. **Recht op verwijdering ('vergetelheid')** – het recht om persoonsgegevens te laten wissen indien daar geen geldige reden meer voor is.
4. **Recht op beperking van de verwerking** – het recht om minder gegevensverwerking te vragen bij een geschil over juistheid of rechtmatigheid.
5. **Recht op overdraagbaarheid (dataportabiliteit)** – het recht om gegevens te ontvangen in een gestructureerd, gangbaar en machineleesbaar formaat.
6. **Recht van bezwaar** – het recht om bezwaar te maken tegen bepaalde verwerkingen, zoals marketing of gerechtvaardigd belang.
7. **Recht op menselijke tussenkomst bij geautomatiseerde besluitvorming** – indien besluiten volledig geautomatiseerd worden genomen.

Verzoeken kunnen worden ingediend via het privacyformulier in Zenya. Beantwoording vindt in principe plaats binnen één maand na ontvangst van het verzoek. Indien nodig kan deze termijn met nog eens één maand worden verlengd, met motivering.

Ingediende verzoeken van betrokkenen worden centraal geregistreerd in Zenya. Hierbij worden de aard van het verzoek, datum van ontvangst, verwerking, eventuele motivering van uitstel en

de reactie aan betrokkene vastgelegd. Dit borgt de verantwoordingsplicht conform artikel 12 AVG en maakt monitoring van de doorlooptijd mogelijk.

6. Verwerkingsregister en grondslagen

Vitaal Zorggroep houdt een verwerkingsregister bij dat een overzicht bevat van alle processen waarbij persoonsgegevens worden verwerkt. Dit register is:

- Verplicht onder de AVG (artikel 30);
- Jaarlijks geactualiseerd onder toezicht van de Privacy Officer en FG;
- Per verwerking voorzien van:
  - Doel van de verwerking;
  - Categorieën persoonsgegevens en betrokkenen;
  - Verwerkingsgrondslag (zoals overeenkomst, wettelijke verplichting);
  - Ontvangers van gegevens (zoals verwerkers);
  - Bewaartermijnen;
  - Passende technische en organisatorische maatregelen.

De gebruikte verwerkingsgrondslagen binnen Vitaal Zorggroep zijn:

- Toestemming van de betrokkene (bijvoorbeeld bij nieuwsbrieven);
- Uitvoering van een overeenkomst (zoals de zorgovereenkomst);
- Wettelijke verplichting (zoals fiscale bewaarplicht);
- Vitaal belang (bijvoorbeeld bij medische noodsituaties);
- Taak van algemeen belang (zoals meldingen aan inspecties);
- Gerechtvaardigd belang (bijvoorbeeld interne kwaliteitscontrole, mits belangenafweging is gemaakt).

Vitaal Zorggroep hanteert bewaartermijnen die zijn afgestemd op wet- en regelgeving. Voor de meest voorkomende gegevenscategorieën gelden de volgende richtlijnen:

Categorie gegevens	**Bewaartermijn**	**Wettelijke grondslag / toelichting**
Cliëntendossier	15 jaar	WGBO, art. 7:454 lid 3 BW
Personeelsdossier	7 jaar na uitdiensttreding	Belastingwetgeving
Sollicitatiegegevens	4 weken (of 1 jaar bij toestemming)	AVG, Beleidsregels werving & selectie
Financiële administratie	7 jaar	Wet op de Rijksbelastingen
Camerabeelden (indien van toepassing)	Maximaal 4 weken	AVG, tenzij incident of onderzoek

Nieuwsbriefgegevens	Tot uitschrijving	Toestemming betrokkene

Vitaal Zorggroep verwerkt persoonsgegevens in beginsel uitsluitend binnen de Europese Economische Ruimte (EER). Indien doorgifte naar landen buiten de EER noodzakelijk is, worden uitsluitend verwerkers ingezet die passende waarborgen bieden. Dit gebeurt op basis van:

- Een adequaatheidsbesluit van de Europese Commissie;
- Standard Contractual Clauses (SCC's) van de Europese Commissie; of
- Andere waarborgen conform artikel 46 AVG.

Voorbeelden kunnen zijn: gebruik van internationale cloudleveranciers. De Privacy Officer beoordeelt deze situaties vooraf en borgt dat verwerking voldoet aan de eisen van de AVG. Structurele internationale doorgifte is op dit moment niet van toepassing.

7. DPIA (Data Protection Impact Assessment)

Voor verwerkingen die waarschijnlijk een hoog privacyrisico inhouden voor betrokkenen, is een DPIA verplicht. Dit geldt bijvoorbeeld voor:

- Grootschalige verwerking van bijzondere persoonsgegevens (zoals medische gegevens);
- Systematische monitoring (zoals cameratoezicht);
- Nieuwe technologieën (zoals apps voor digitale zelfzorg);
- Verwerkingen met een grote impact op rechten en vrijheden van betrokkenen.

Binnen Vitaal Zorggroep worden DPIA's:

- Uitgevoerd voorafgaand aan de start van een nieuwe verwerking;
- Gecoördineerd door de Privacy Officer, met ondersteuning van de FG;
- Vastgelegd inclusief risicobeoordeling en maatregelen ter beperking van risico's;
- Herhaald indien de aard van de verwerking verandert.

In 2025 staan DPIA's gepland voor:

- Het gebruik van privéapparatuur (telefoons, laptops);
- Beveiliging en logging van cliëntsystemen;
- Nieuwe zorgtoepassingen zoals e-health platforms.

De uitkomsten van een DPIA worden besproken in het Privacy-team en leiden tot concrete verbetermaatregelen.

8. Privacy by Design & Default

Privacy by Design en Privacy by Default zijn verplichte uitgangspunten bij de ontwikkeling en inrichting van systemen, processen en werkwijzen die persoonsgegevens verwerken.

- **Privacy by Design** betekent dat privacybescherming structureel wordt meegenomen vanaf het eerste ontwerpstadium van een proces of systeem.
- **Privacy by Default** houdt in dat standaardinstellingen zo zijn ingericht dat alleen de strikt noodzakelijke persoonsgegevens worden verzameld, gebruikt en bewaard.

Voorbeelden van toepassing binnen Vitaal Zorggroep:

- Automatisch afschermen van niet-noodzakelijke velden in cliëntsystemen.
- Beperkte standaardtoegang op basis van functie (autorisatiematrix).
- Alleen noodzakelijke velden in digitale formulieren.

Deze principes zijn verankerd in het beleidsdocument ‘Beleid Informatiebeveiliging Vitaal Zorggroep’, dat ook voorziet in technische borging zoals encryptie, logging, toegangsbeheer en periodieke evaluaties.

9. Informatiebeveiliging (NEN7510)

Het waarborgen van de veiligheid van informatie is essentieel om persoonsgegevens te beschermen tegen ongeoorloofde toegang, verlies of wijziging. Vitaal Zorggroep volgt de norm NEN7510, die specifiek gericht is op informatiebeveiliging in de zorg.

De uitgangspunten zijn uitgewerkt in het ‘Beleid Informatiebeveiliging Vitaal Zorggroep’ en omvatten:

Toepassing van technische en organisatorische maatregelen, waaronder:

- Firewalls en antivirussoftware;
- Versleuteling van communicatie en bestanden;
- Fysieke beveiliging van werkplekken;
- Logging en monitoring van toegang tot persoonsgegevens.

Inrichting van een Information Security Management System (ISMS), met:

- Rollen en verantwoordelijkheden voor informatieveiligheid;
- Periodieke risicoanalyses;
- Beleid voor mobiele apparaten, wachtwoorden en back-ups;

- Incidentmanagement en herstelprocedures.

Controle en toetsing

- Jaarlijkse interne audits en toetsing op naleving van beleid;
- Inzet van externe deskundigheid indien nodig;
- Rapportages aan bestuur en betrokken toezichthouders.

Voor de implementatie, evaluatie en actualisatie van deze maatregelen wordt verwezen naar het document ‘Beleid Informatiebeveiliging Vitaal Zorggroep’ (beschikbaar via Zenya).

10. Datalekken

Vitaal Zorggroep hanteert een strikt beleid rondom datalekken, in lijn met de AVG en het Beleid Datalekken. Een datalek betreft elke inbreuk op de beveiliging waarbij persoonsgegevens verloren gaan of ongeoorloofd worden ingezien, gewijzigd of verspreid.

De procedure bij een (vermoedelijk) datalek:

1. **Melding**: Medewerkers melden incidenten direct via Zenya Flow.
2. **Beoordeling**: Het Datalek-team (Privacy Officer en FG) beoordeelt het incident binnen 24 uur.
3. **Classificatie**: Er wordt bepaald of sprake is van een datalek en of melding aan de Autoriteit Persoonsgegevens (AP) vereist is.
4. **Melding aan AP**: Bij meldingsplicht wordt het lek binnen 72 uur na ontdekking gemeld.
5. **Informatie aan betrokkene**: Indien het lek waarschijnlijk een hoog risico oplevert voor de rechten van betrokkenen, worden zij geïnformeerd.
6. **Registratie**: Alle meldingen en genomen maatregelen worden geregistreerd in het datalekregister.
7. **Evaluatie**: Er wordt geëvalueerd welke structurele maatregelen nodig zijn om herhaling te voorkomen.

Deze aanpak is vastgelegd in het beleidsdocument **'Beleid Datalekken'** en wordt jaarlijks geëvalueerd.

De afhandeling van datalekken is onderdeel van het bredere incidentmanagementsysteem van Vitaal Zorggroep. Incidenten worden niet alleen geregistreerd als datalek, maar ook beoordeeld op bredere risico's (bijv. cliëntveiligheid, continuïteit zorg). Er is afstemming met calamiteitenbeleid en kwaliteitsmanagement. Evaluaties van datalekken kunnen leiden tot structurele verbeteracties binnen meerdere domeinen.

11. Verwerkers en overeenkomsten

Vitaal Zorggroep maakt gebruik van verwerkers die in opdracht persoonsgegevens verwerken, zoals softwareleveranciers, arbodiensten of administratieve dienstverleners. Met deze partijen worden verwerkersovereenkomsten gesloten waarin minimaal de volgende zaken zijn geregeld:

- De aard en het doel van de verwerking;
- De soorten persoonsgegevens en categorieën betrokkenen;
- De duur van de verwerking;
- De rechten en verplichtingen van Vitaal Zorggroep als verwerkingsverantwoordelijke;
- Technische en organisatorische beveiligingsmaatregelen;
- Geheimhoudingsplicht;
- Ondersteuning bij datalekken, DPIA's en uitoefening van rechten van betrokkenen;
- Subverwerkers en doorverplichtingen;
- Teruggeven of vernietigen van gegevens na afloop van de overeenkomst.

De Privacy Officer beheert het overzicht van actieve verwerkers en toetst jaarlijks of:

- De overeenkomsten nog actueel en volledig zijn;
- Er wijzigingen zijn in het type verwerking of gebruikte systemen;
- Er nieuwe verwerkers zijn toegevoegd.

Voorbeeldovereenkomsten zijn beschikbaar via Zenya en zijn afgestemd op de AVG en het model van de brancheorganisatie.

Voor elke (sub)verwerker geldt dat Vitaal Zorggroep aantoonbaar heeft beoordeeld of deze partij voldoende garanties biedt op het gebied van informatiebeveiliging en naleving van de AVG. Hierbij wordt onder andere gekeken naar ISO/NEN-certificeringen, het beveiligingsbeleid, incidentprocedures, en ervaring in de zorgsector. Deze beoordeling wordt voorafgaand aan contractsluiting gedaan én periodiek herhaald (minimaal 1x per 2 jaar).

Vitaal Zorggroep verwerkt gegevens in principe uitsluitend binnen de EU/EER. Indien sprake is van gegevensopslag of verwerking buiten de EU (bijvoorbeeld via clouddiensten), wordt uitsluitend samengewerkt met partijen die passende waarborgen bieden (zoals Standard

Contractual Clauses of adequaatheidsbesluiten). Deze situaties worden vastgelegd in het verwerkingsregister en expliciet opgenomen in de verwerkersovereenkomst.

12. Bewustwording en training

Het creëren van een privacybewuste organisatiecultuur is een continue opgave. Vitaal Zorggroep investeert structureel in het vergroten van kennis, houding en gedrag rondom privacy en informatieveiligheid. Dit gebeurt op meerdere niveaus:

- **Privacyteam:** Komt tweemaandelijks bijeen om signalen, ontwikkelingen en risico's te bespreken en acties te coördineren.
- **E-learnings:** Jaarlijks verplichte e-learningmodules voor alle medewerkers, inclusief toetsing.
- **Workshops en trainingen:** Gerichte bijeenkomsten voor aandachtsvelders, teamleiders en nieuwe medewerkers.
- **Communicatie:** Regelmatige updates in de interne nieuwsbrief, het intranet en Zenya over actuele thema's en tips.
- **Inwerkprogramma's:** Privacy en gegevensbescherming maken standaard deel uit van onboarding.

Iedere medewerker is verantwoordelijk voor het naleven van het beleid en heeft de plicht om signalen of incidenten te melden.

13. Toestemming en informatievoorziening

Vitaal Zorggroep verwerkt persoonsgegevens op basis van heldere grondslagen. In gevallen waar toestemming vereist is, wordt deze:

- Actief en geïnformeerd verkregen (bijvoorbeeld voor nieuwsbrieven, foto's, gebruik van apps);
- Vastgelegd in het cliënt- of personeelsdossier;
- Herroepbaar op elk gewenst moment, zonder nadelige gevolgen.

Informatievoorziening aan betrokkenen gebeurt via:

- De privacyverklaring voor cliënten en medewerkers (beschikbaar op de website en in Zenya);
- Schriftelijke en mondelinge toelichting bij intakegesprekken of arbeidscontracten;
- De algemene voorwaarden en zorg-/arbeidsovereenkomsten.

In alle communicatie wordt gestreefd naar begrijpelijke en toegankelijke taal, afgestemd op de doelgroep.

Voor minderjarige cliënten of cliënten die wilsonbekwaam zijn, wordt toestemming gevraagd aan de wettelijk vertegenwoordiger (zoals ouder, voogd of curator), conform de Wet op de geneeskundige behandelingsovereenkomst (WGBO). Informatievoorziening en uitoefening van rechten zoals inzage, rectificatie en vergetelheid verloopt eveneens via deze vertegenwoordiger, tenzij de cliënt zelf wilsbekwaam wordt geacht voor dat specifieke onderwerp. Deze werkwijze is ook van toepassing op cliënten die onder mentorschap of curatele staan.

14. Toezicht en naleving

Toezicht op de naleving van de AVG en dit beleid vindt op verschillende niveaus plaats:

- Functionaris Gegevensbescherming (FG): Onafhankelijke toezichthouder die adviseert, toetst en rapporteert.
- Privacy Officer: Coördineert de uitvoering van beleid, verzorgt rapportages en initieert verbeteracties.
- Interne audits: Jaarlijks uitgevoerd, inclusief steekproeven en gesprekken op locatie.
- Controle door lijnmanagement: Directie is verantwoordelijk voor implementatie en naleving binnen de organisatieonderdelen.
- Externe toetsing: Bijvoorbeeld in het kader van NEN7510-audits of inspectiebezoeken.

Bevindingen uit audits en meldingen worden vertaald naar verbetermaatregelen en waar nodig besproken in het privacyteam en het DT.

15. Evaluatie en actualisatie

Het AVG-beleid wordt:

- Jaarlijks geëvalueerd door de Privacy Officer en FG;
- Bijgesteld op basis van wet- en regelgeving, interne ontwikkelingen, incidenten of aanbevelingen uit audits;
- Voorgelegd aan het bestuur ter goedkeuring;
- Verspreid via Zenya en besproken tijdens management- en privacyteamoverleggen.

De evaluatie wordt vastgelegd in het Jaarplan Privacy en Informatiebeveiliging. Feedback vanuit de organisatie wordt actief verzameld en meegenomen bij herziening.

16. Samenvatting/ Kernboodschap

- Dit beleid helpt om privacyrisico's te beheersen, te voldoen aan wetgeving en bewustwording te vergroten binnen alle onderdelen van Vitaal Zorggroep.
- Medewerkers worden geacht om zorgvuldig en verantwoordelijk om te gaan met persoonsgegevens, signalen en datalekken tijdig te melden en zich aan de afspraken in dit beleid te houden.
- In geval van twijfel of vragen over gegevensverwerking kunnen medewerkers terecht bij de Privacy Officer of de Functionaris Gegevensbescherming.
- Privacy is een gedeelde verantwoordelijkheid: iedereen binnen de organisatie draagt bij aan de bescherming van persoonsgegevens.
- Gebruik Zenya als bron voor de meest actuele informatie, formulieren en beleidsdocumenten rondom privacy en informatieveiligheid.

Alle medewerkers, vrijwilligers, zzp'ers en externe partners dienen op de hoogte te zijn van dit beleid. Onze kernboodschap luidt:

Privacy is geen papieren werkelijkheid, maar dagelijkse praktijk. Door bewust om te gaan met persoonsgegevens, beschermen we de rechten van cliënten, collega's en anderen, bouwen we samen aan vertrouwen.

Bijlagen

1. Rollen en verantwoordelijkheden AVG

Bijlage 1: Overzicht rollen en verantwoordelijkheden

OVERZICHT ROLLEN EN VERANTWOORDELIJKHEDEN		
Functie	Rol	Verantwoordelijkheden
Bestuur/ Directie	Eindverantwoordelijke voor privacy en gegevensbescherming.	Vaststellen van privacybeleid en strategie. Beschikbaar stellen van middelen en capaciteit voor privacymaatregelen en prioriteren bewustwordingsactiviteiten. Toezien op implementatie en naleving van de AVG, NEN7510 en interne privacyprocedures. Periodiek evalueren van effectiviteit en risico's op bestuurlijk niveau. Voorbeeldgedrag tonen (bijv. zelf trainingen volgen, beleid naleven). Uitdragen van 'privacy by design & default'-principe.
Functionaris Gegevensbescherming (FG)	Onafhankelijk toezichthouder op gegevensbescherming.	Toezien op naleving van de AVG en andere privacywetgeving. Adviseren van bestuur en management over privacyverplichtingen. Toezicht houden op uitvoering van DPIA's (Data Protection Impact Assessments). Fungeren als contactpersoon voor de Autoriteit Persoonsgegevens en betrokkenen. Onafhankelijk kunnen functioneren binnen de organisatie.
Privacy Officer (PO)	Coördinator en uitvoerder van het privacybeleid.	Coördineren van het privacyprogramma binnen de organisatie. Opstellen, actualiseren en implementeren van het privacybeleid. Bewaken van uitvoering van maatregelen en richtlijnen. Ondersteunen van het management en medewerkers bij vragen of knelpunten. Melden en opvolgen van datalekken in samenwerking met FG. Voorzitten en coördineren van het privacyteam. Ontwikkelen en implementeren van het privacybewustzijnsprogramma. Opstellen en coördineren van trainingen, e-learnings, campagnes en interne communicatie.
Privacyteam	Team voor afstemming en borging van privacy over alle organisatieonderdelen.	Periodiek overleg over privacy risico's, maatregelen en incidenten. Adviseren over en ondersteunen bij DPIA's en datalekken. Stimuleren van kennisdeling en eenduidige toepassing van privacybeleid. Signaleren van ontwikkelingen en benodigde beleidsaanpassingen. Bevorderen van samenwerking tussen PO, FG, ICT, juridische zaken en aandachtsveldjes.

Aandachtsvelders Privacy (per team/locatie/afdeling)	Lokaal aanspreekpunt voor privacy.	Signaleren van risico's en knelpunten binnen het eigen team. Signaleren van onduidelijkheden of onjuist gedrag en dit bespreekbaar maken. Bevorderen van privacybewustzijn onder collega's. Toezien op naleving van privacyprocedures op de werkvloer. Informeren van PO over relevante signalen en incidenten. Ondersteunen bij het organiseren van privacytrainingen en -acties.
Medewerkers	Verantwoordelijke voor zorgvuldige omgang met persoonsgegevens in het dagelijks werk.	Naleven van het privacybeleid, procedures en gedragsregels. Correct verwerken, bewaren en delen van persoonsgegevens. Melden van datalekken of incidenten via de vastgestelde route. Volgen van verplichte trainingen over privacy en informatiebeveiliging. Actieve bijdrage aan het beschermen van privacy binnen de organisatie.

Bijlagen en verdiepingsinformatie

A. Toepassingsgebied

Dit beleid is van toepassing op alle onderdelen van Vitaal Zorggroep, inclusief:

- Medewerkers, vrijwilligers, stagiairs, uitzendkrachten en zzp'ers;
- Teams in zorg, ondersteuning, bedrijfsvoering en management;
- Alle locaties van Vitaal Zorggroep en haar dochtermaatschappijen;
- Alle processen waarbij persoonsgegevens worden verwerkt (bijv. zorgverlening, personeelszaken, ICT, financiën en communicatie).

B. Definities

- **AVG:** Algemene Verordening Gegevensbescherming.
- **Persoonsgegevens:** Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
- **Verwerking:** Elke bewerking van persoonsgegevens, zoals verzamelen, opslaan, raadplegen, wijzigen, verstrekken of verwijderen.
- **Betrokkene:** De persoon op wie de persoonsgegevens betrekking hebben.
- **FG:** Functionaris Gegevensbescherming, onafhankelijk toezichthouder binnen de organisatie.
- **DPIA:** Data Protection Impact Assessment, risicoanalyse bij nieuwe of risicovolle verwerkingen.
- **Zenya:** Het kwaliteitssysteem waarin beleid, meldformulieren, procedures en registraties worden vastgelegd en gedeeld.

C. Risico's en Beheersmaatregelen

Risico's bij het niet naleven van dit beleid:

- Ongeautoriseerde toegang tot vertrouwelijke gegevens;
- Datalekken en verlies van persoonsgegevens;
- Schade aan cliënten of medewerkers (bijv. verlies privacy, reputatieschade);
- Sancties of boetes vanuit de Autoriteit Persoonsgegevens;
- Vertrouwensverlies bij cliënten, medewerkers en samenwerkingspartners.

Beheersmaatregelen:

- Heldere richtlijnen en bewustwordingstrainingen voor medewerkers;
- Technische beveiliging (zoals toegangscontrole, encryptie en logging);

- Aanstelling van FG, Privacy Officer en aandachtsvelders privacy;
- Actueel verwerkingsregister en beleid datalekken;
- DPIA's voor risicovolle verwerkingen;
- Interne audits en periodieke evaluaties.

D. Verwijzingen

Relevante wet- en regelgeving:

- Algemene Verordening Gegevensbescherming (EU) 2016/679 (AVG);
- Uitvoeringswet AVG (UAVG);
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz);
- NEN7510: Norm voor informatiebeveiliging in de zorgsector;
- Wet op de geneeskundige behandelingsovereenkomst (WGBO);
- Arbeidsomstandighedenwet (Arbowet) – m.b.t. persoonsgegevens van personeel.

Interne protocollen of andere documenten (Zenya):

- Beleid informatiebeveiliging
- Beleid datalekken
- Privacyverklaring cliënten
- Privacyverklaring medewerker & sollicitant
- Format Verwerkingsregister
- Beleid Datalekken
- Jaarplan en -planning Privacy en Informatiebeveiliging 2025-2026
- Verwerkingsregister

E. Documentbeheer

Auteur: Emete Solmaz

Datum: 17-06-2025

Versie: 1.0

Goedkeurder: Beleid & Kwaliteit

Herzieningsdatum: 17-06-2027