

Privacyreglement Kennemerhart

Maart 2026

Functionaris Gegevensbescherming:
Anat Fuldauer
privacy@kennemerhart.nl

Verantwoordelijk bestuurders:
Joke Hoekstra & Sander Hofstede

Samenvatting

Bij Kennemerhart vinden we privacy net zo belangrijk als goede zorg. We doen er alles aan om uw persoonlijke gegevens veilig te houden en duidelijk uit te leggen wat we ermee doen. Wanneer u bij ons zorg ontvangt, hebben we bepaalde informatie van u nodig, zoals uw naam, adres en contactgegevens. Ook bewaren we medische gegevens, zoals diagnoses en behandelplannen, zodat we u de juiste zorg kunnen geven. Soms verwerken we ook financiële gegevens, bijvoorbeeld voor declaraties, en informatie van familie of mantelzorgers om goed met hen te kunnen overleggen.

We gebruiken deze gegevens voor het leveren van zorg, het nakomen van wettelijke verplichtingen en om onze dienstverlening te verbeteren. Daarbij zorgen we voor strenge beveiliging: onze systemen zijn goed beschermd, alleen bevoegde medewerkers hebben toegang en papieren dossiers worden veilig opgeborgen. Als er toch iets misgaat, melden we dat direct en nemen maatregelen.

Gegevens bewaren we niet langer dan nodig. Zo blijft een medisch dossier twintig jaar bewaard na de laatste behandeling, financiële gegevens zeven jaar en camerabeelden maximaal vier weken. We delen uw gegevens alleen met zorgverleners die bij uw behandeling betrokken zijn of met instanties als de wet dat verplicht. Nooit zonder reden en nooit meer dan nodig.

U heeft altijd het recht om te weten welke gegevens we hebben, om ze in te zien, fouten te laten corrigeren of (als de wet dat toestaat) te laten verwijderen. U kunt ook bezwaar maken tegen het gebruik van uw gegevens.

Heeft u vragen of wilt u een verzoek indienen? Dan kunt u contact opnemen met onze Functionaris Gegevensbescherming:

Anat Fuldauer
privacy@kennemerhart.nl

Meer informatie vindt u ook op www.autoriteitpersoonsgegevens.nl.

Inhoud

Samenvatting	1
1 Inleiding	4
1.1 Doel van het privacyreglement	4
1.2 Toepassingsgebied	4
1.3 Uitgangspunten voor gegevensverwerking	4
1.4 Wettelijk kader	5
1.5 Verantwoordelijkheid en toezicht	5
1.6 Communicatie en bekendmaking	5
1.7 Evaluatie en actualisatie	5
2 Begripsbepalingen	6
3 Soorten gegevens en categorieën van betrokkenen	8
3.1 Algemeen uitgangspunt	8
3.2 Categorieën van betrokkenen	8
3.3 Categorieën van persoonsgegevens	8
3.4 Herkomst van de gegevens	9
3.5 Bewaartermijnen per categorie	9
3.6 Nauwkeurigheid en actualiteit	10
3.7 Pseudonimisering en anonimisering	10
4 Doeleinden van de gegevensverwerking	11
4.1 Algemeen uitgangspunt	11
4.2 Primaire doeleinden: Zorgverlening	11
4.3 Secundaire doeleinden: Organisatie en kwaliteit van zorg	12
4.4. Beveiliging, incidentenbeheer en toezicht	12
4.5 Gebruik voor andere doeleinden	12
5 Grondslagen van de verwerking	13
5.1 Algemeen uitgangspunt	13
5.2 Grondslagen op grond van de AVG	13
5.3 Verwerking van bijzondere persoonsgegevens (gezondheidsgegevens)	14
5.4 Verhouding tot de WGBO en Wabvpz	14
5.5 Documentatieplicht en verantwoording	14
6 Beveiliging van persoonsgegevens	15
6.1 Algemeen uitgangspunt	15
6.2 Beveiligingsbeleid en verantwoordelijkheden	15
6.3 Technische beveiligingsmaatregelen	16
6.4 Datalekken en incidentenmanagement	16

7 Digitale Zorgtoepassingen.....	17
7.1 Algemeen uitgangspunt.....	17
7.2 Technologieën in gebruik.....	17
7.3 Voorwaarden voor gebruik.....	17
7.4 Waarborging van privacy en autonomie.....	17
8 Delen van persoonsgegevens met derden.....	18
8.1 Algemeen uitgangspunt.....	18
8.2 Wettelijke grondslagen voor gegevensdeling.....	18
8.3 Delen van gegevens binnen de zorgketen.....	18
8.4 Delen van gegevens met mantelzorgers en familie.....	19
8.5 Delen van gegevens met externe partijen (verwerkers en derden).....	19
8.6 Wettelijk meld- en rapportageverplichtingen.....	20
8.7 Gegevensdeling in elektronische zorgsystemen.....	20
8.8 Delen van gegevens met toezichthouders, politie of justitie.....	20
8.9 Geanonimiseerde of gepseudonimiseerde gegevens.....	20
8.10 Transparantie over gegevensdeling.....	20
9 Rechten van betrokkenen.....	22
9.1 Algemeen uitgangspunt.....	22
9.2 Categorieën van betrokkenen met rechten.....	22
9.3 Overzicht van rechten onder de AVG.....	22
9.4 Procedure voor uitoefening van rechten.....	23
9.5 Beperkingen op grond van andere wetgeving.....	23
9.6 Uitoefening van rechten door vertegenwoordigers.....	23
9.7 Klachten en geschillen.....	23
9.9 Transparantie & communicatie.....	24
10 Kunstmatige Intelligentie (AI).....	25
10.1 Algemeen uitgangspunt.....	25
10.2 Transparantie en menselijke controle.....	25
10.3 Gegevensverwerking en privacy.....	25
10.4 Ethisch kader en zorgvuldigheid.....	25
10.5 Toezicht en evaluatie.....	25
11 Gebruik van data-analyse en big data.....	26
11.1 Doel en uitgangspunten.....	26
11.2 Waarborgen.....	26
Bijlage: Toelichting Bij Privacyreglement: Stand van zaken.....	27

1 Inleiding

1.1 Doel van het privacyreglement

Het doel van dit privacyreglement is om vast te leggen op welke wijze Kennemerhart omgaat met persoonsgegevens van cliënten, medewerkers, vrijwilligers, stagiaires en andere betrokkenen.

Binnen Kennemerhart worden dagelijks persoonsgegevens verwerkt om goede, veilige en verantwoorde zorg te bieden. Wij vinden het van groot belang dat met deze gegevens zorgvuldig wordt omgegaan en dat de privacy van alle betrokkenen wordt beschermd.

Met dit reglement voldoen wij aan de verplichtingen die voortvloeien uit de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG) en de relevante zorgwetgeving. Daarnaast willen wij cliënten en medewerkers duidelijk informeren over hun rechten en de wijze waarop zij deze kunnen uitoefenen.

Het privacyreglement heeft tot doel:

- Te waarborgen dat persoonsgegevens op een rechtmatige, behoorlijke en transparante manier worden verwerkt.
- Inzicht te geven in de soorten gegevens die worden verwerkt en de doeleinden daarvan.
- Duidelijkheid te verschaffen over de verantwoordelijkheden binnen de organisatie.
- De rechten van betrokkenen te waarborgen.
- Te beschrijven welke technische en organisatorische maatregelen worden getroffen om gegevens te beveiligen.

1.2 Toepassingsgebied

Dit privacyreglement is van toepassing op alle verwerkingen van persoonsgegevens die plaatsvinden binnen Kennemerhart, ongeacht de vorm of het medium waarop deze gegevens worden vastgelegd (digitaal, schriftelijk of mondeling)

Het reglement geldt voor:

- Alle cliënten die zorg of ondersteuning ontvangen van Kennemerhart.
- Alle medewerkers, stagiaires, vrijwilligers en ingehuurd krachten.
- Externe partijen die in opdracht van de organisatie persoonsgegevens verwerken (verwerkers).

Het reglement is van toepassing op alle vormen van zorgverlening, waaronder woonzorglocaties, zorg aan huis, dag- en ontmoetingscentra, begeleiding & ondersteuning en overige diensten die organisatie aanbiedt.

1.3 Uitgangspunten voor gegevensverwerking

Bij de verwerking van persoonsgegevens hanteert Kennemerhart de volgende uitgangspunten, conform de AVG:

1. Rechtmatigheid, behoorlijkheid en transparantie: Gegevens worden op een eerlijke en begrijpelijke manier verwerkt, met respect voor de rechten van betrokkene.
2. Doelbinding: Gegevens worden uitsluitend verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
3. Dataminimalisatie: Alleen die gegevens worden verwerkt die noodzakelijk zijn voor het doel van de verwerking.
4. Juistheid: Gegevens worden actueel gehouden en waar nodig gecorrigeerd.
5. Opslagbeperking: Gegevens worden niet langer bewaard dan noodzakelijk is.

6. Integriteit en vertrouwelijkheid: Gegevens worden beschermd tegen onbevoegde of onrechtmatige verwerking en tegen verlies, vernietiging of beschadiging.
7. Verantwoordingsplicht: De organisatie kan aantonen dat zij aan bovenstaande beginselen voldoet.

1.4 Wettelijk kader

De verwerking van persoonsgegevens binnen Kennemerhart vindt plaats binnen de kaders van de volgende wet- en regelgeving:

- Algemene Verordening Gegevensbescherming (AVG)
- Uitvoeringswet AVG (UAVG)
- Wet op geneeskundige behandelingsovereenkomst (WGBO)
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)
- Wet kwaliteit, klachten en geschillen zorg (Wkkgz)
- Wet gebruik Burgerservicenummer in de zorg (Wbsn-z)
- Wet elektronische gegevensuitwisseling in de zorg (Wegiz)
- NEN7510, 7512 en 7513, normen voor informatiebeveiliging en logging in de zorg
- Europese NIS2-richtlijn
- De EU AI act

Waar deze wetten en normen specifieke verplichtingen bevatten (zoals bewaartermijnen, rechten van cliënten of technische beveiligingsmaatregelen), worden deze in de volgende hoofdstukken nader uitgewerkt.

1.5 Verantwoordelijkheid en toezicht

De verwerkingsverantwoordelijke in de zin van de AVG is Kennemerhart, vertegenwoordigd door het bestuur. Het bestuur is eindverantwoordelijk voor de naleving van de privacywetgeving en dit reglement.

De organisatie heeft een Functionaris Gegevensbescherming (FG) aangewezen die toezicht houdt op de naleving van de AVG, adviseert over privacyvraagstukken en als aanspreekpunt fungeert voor cliënten, medewerkers en de Autoriteit Persoonsgegevens (AP).

Contactgegevens FG
Anat Fuldauer
privacy@kennemerhart.nl

1.6 Communicatie en bekendmaking

Dit privacyreglement wordt intern en extern beschikbaar gesteld, onder meer via het internet, de website en op verzoek in papieren vorm.

1.7 Evaluatie en actualisatie

De inhoud van dit privacyreglement wordt minimaal één keer per twee geëvalueerd en waar nodig aangepast aan wijzigingen in wet- en regelgeving, beleid of organisatieprocessen. Wijzigingen worden vastgesteld door het bestuur en gecommuniceerd aan medewerkers en cliënten.

2 Begripsbepalingen

Om dit privacyreglement eenduidig te maken, worden in dit hoofdstuk de belangrijkste begrippen gedefinieerd. Deze definities zijn gebaseerd op de AVG, de Wabvpz de WGBO, en de NEN-normen voor informatiebeveiliging.

Een persoonsgegeven:

Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de “Betrokkene”). (Bron: AVG)

Bijzondere persoonsgegevens:

Gegevens die extra bescherming nodig hebben vanwege hun gevoeligheid. In de ouderenzorg gaat het vooral om gezondheidsgegevens en gegevens over afkomst, religie, levensovertuiging en seksuele geaardheid. (Bron: AVG & Wabvpz)

Verwerking:

Verwerking betekent elke bewerking van persoonsgegevens, zoals verzamelen, registreren, opslaan, wijzigen, raadplegen, gebruiken, doorgeven, archiveren of vernietigen. (Bron: AVG)

Verwerkingsverantwoordelijke:

De verwerkingsverantwoordelijke is degene die het doel en de middelen van de verwerking bepaalt. Bij Kennemerhart is dit het bestuur van de organisatie. (Bron: AVG)

Verwerker:

Een verwerker verwerkt persoonsgegevens namens de verwerkingsverantwoordelijke. (Bron: AVG)

Betrokkene:

De betrokkene is de natuurlijke persoon van wie de persoonsgegevens worden verwerkt. Het gaat bij Kennemerhart onder andere om cliënten, medewerkers, vrijwilligers en mantelzorgers. (Bron: AVG)

Derde:

Elke persoon of instantie die geen betrokkene, verwerkingsverantwoordelijke, verwerker of persoon is die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is persoonsgegevens te verwerken.

Toestemming:

Toestemming is een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene instemt met de verwerking van zijn/haar persoonsgegevens. (Bron: AVG)

Dossier/Zorgdossier:

Een Zorgdossier is een verzameling van persoonsgegevens die verband houden met de zorg en behandeling van een cliënt. Dit kan bestaan uit medische gegevens, behandelplannen observaties, rapportages, correspondentie met zorgverleners of familie. (Bron: WGBO, Wabvpz & NEN)

Elektronisch Cliëntendossier (ECD):

Een ECD is het digitale equivalent van het zorgdossier, waarin alle relevantie informatie over een cliënt elektronisch wordt opgeslagen en beveiligd. (Bron: Wegiz, AVG en NEN)

Datalek

Een datalek is een inbreuk op de beveiliging van persoonsgegevens waardoor deze verloren gaan, vernietigd worden, onbevoegd worden ingezien, gewijzigd of verspreid. (Bron: AVG)

Pseudonimisering:

Een beveiligingstechniek waarbij persoonsgegevens worden verwerkt op zodanige wijze dat ze niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder aanvullende informatie, die apart en beveiligd wordt bewaard (Bron: AVG)

Functionaris Gegevensbescherming (FG):

De FG is verantwoordelijk voor het toezicht op de naleving van de privacyregels, het adviseren van het bestuur, en het aanspreekpunt zijn voor betrokkenen en de Autoriteit Persoonsgegevens. (Bron: AVG)

Verwerkersovereenkomst:

Een verwerkersovereenkomst is een schriftelijke overeenkomst tussen de verwerkingsverantwoordelijke en een verwerker waarin afspraken worden vastgelegd over de verwerking van persoonsgegevens, de beveiliging en de verantwoordelijkheden. (Bron: AVG)

Bewaartermijn:

De bewaartermijn is de periode waarin persoonsgegevens worden bewaard, rekening houdend met wettelijke verplichtingen en organisatorische of beleidsmatige redenen. (Bron: AVG)

Geautomatiseerde besluitvorming:

Elke beslissing die volledig automatisch wordt genomen op basis van persoonsgegevens, zonder menselijke tussenkomst. (Bron: AVG)

Artificial Intelligence/kunstmatige intelligentie (AI):

Technologie die gebruikmaakt van algoritmen en data-analyse om patronen te herkennen, voorspellingen te doen of beslissingen te ondersteunen. Binnen Kennemerhart wordt AI uitsluitend ingezet ter ondersteuning van zorg en bedrijfsvoering, met behoud van menselijke controle. (AI act)

3 Soorten gegevens en categorieën van betrokkenen

3.1 Algemeen uitgangspunt

Kennemerhart verwerkt uitsluitend persoonsgegevens die noodzakelijk zijn voor de uitvoering van haar zorg- en bedrijfsactiviteiten. Er worden niet meer gegevens verzameld dan strikt nodig voor het doel waarvoor ze worden verwerkt, in overeenstemming met het dataminimalisatiebeginsel (Bron: AVG)

De aard en gevoeligheid van de gegevens verschillen per categorie betrokkene (zoals cliënten, medewerkers of vrijwilligers). Voor iedere categorie gelden passende beveiligingsmaatregelen.

3.2 Categorieën van betrokkenen

Binnen Kennemerhart worden persoonsgegevens verwerkt van de volgende groepen betrokkenen:

- Cliënten en/of bewoners
- Wettelijke vertegenwoordigers, mantelzorgers en contactpersonen
- Medewerkers, vrijwilligers en stagiaires
- Zorgverleners en ketenpartners
- Leveranciers en dienstverleners (verwerkers)
- Bezoekers en relaties

3.3 Categorieën van persoonsgegevens

De organisatie verwerkt de volgende typen gegevens, afhankelijk van de aard van de relatie met de betrokkene:

Algemene persoonsgegevens

- Naam, adres, woonplaats (NAW-gegevens)
- Geboortedatum, geslacht, burgerlijke staat
- BSN
- Contactgegevens
- Taalvoorkeur en correspondentiegeschiedenis

Doel: Identificatie, communicatie, administratie en uitvoering van de zorg- of arbeidsovereenkomst.

Wettelijke basis: AVG & Wbsn-z.

Medische en zorginhoudelijke gegevens (bijzondere persoonsgegevens)

- Diagnoses, behandel- en zorgplannen
- Medicatie- en allergiegegevens
- Observaties, rapportages en voorgangsverslagen
- Functiebeperkingen, valrisico's, voedingstoestand, ADL-beoordelingen
- Laboratoriumuitslagen, onderzoeksresultaten, verslagen van specialisten
- Indicatiebesluiten

Doel: Veilige en kwalitatieve zorgverlening, behandeling en dossiervorming.

Wettelijke basis: AVG, WGBO & Wabvpz.

Financiële en administratieve gegevens

- Bankrekeningnummer, verzekeringsgegevens, indicaties
- Declaratie- en facturatiegegevens (zorgverzekeraar, CAK, zorgkantoor)
- Betaalhistorie en subsidiestukken

Doel: facturatie, bekostiging en naleving van financiële regelgeving.

Wettelijke basis: AVG, Wkkgz & fiscale wetgeving.

Gegevens van vertegenwoordigers, familie en mantelzorgers

- Naam, relatie tot cliënt, contactinformatie
- Machtigingen of vertegenwoordigingsbewijzen (curatele, mentorschap)
- Informatie relevant voor communicatie en zorgafstemming

Doel: Communicatie, belangenbehartiging en betrokkenheid bij zorgproces.

Wettelijke basis: AVG & WGBO.

Medewerkers- en vrijwilligersgegevens

- Identificatie- en contactgegevens
- Loon- en contractgegevens
- Opleiding, werkervaring, functie, planning
- Verzuim- en re-integratiegegevens (voor zover noodzakelijk)
- Verklaring Omtrent Gedrag (VOG)
- Registraties in BIG-register of kwaliteitsregisters

Doel: Personeelsbeheer, loonadministratie, werving en selectie, scholing en kwaliteit.

Wettelijke basis: AVG, Arbeidswetgeving, Arbowet & Wet BIG.

ICT- en beveiligingsgegevens

- Gebruikersaccounts en loggegevens
- Camerabeelden van gemeenschappelijke ruimten
- Systeemlogbestanden, IP-adressen, e-mail- en inlogsessies.

Doel: Waarborgen van informatiebeveiliging, controle op toegang en incidentenbeheer.

Wettelijke basis: AVG & Wabvpz.

Communicatie- en marketinggegevens

- Nieuwsbriefinschrijvingen
- Contact via formulieren, social media of webcare
- Foto- of beeldmateriaal van activiteiten (alleen met toestemming)

Doel: Informatieverstrekking, betrokkenheid en transparante communicatie.

Wettelijke basis: AVG

3.4 Herkomst van de gegevens

Persoonsgegevens worden verkregen:

- Rechtstreeks van de betrokkene (bij intake of aanmelding)
- Via vertegenwoordigers of mantelzorgers
- Van verwijzers of zorgverleners
- Uit officiële registraties

3.5 Bewaartermijnen per categorie

Kennemerhart bewaart persoonsgegevens niet langer dan noodzakelijk voor het doel van verwerking of wettelijk is voorgeschreven.

Categorie	Bewaartermijn	Wettelijke grondslag
Medisch dossier	20 jaar na laatste behandeling	WGBO
Financiële administratie	7 jaar	Algemene wet inzake rijksbelastingen
Camerabeelden	Maximaal 4 weken (tenzij incident)	AVG

Sollicitatiegegevens	Maximaal 4 weken na afloop van procedure (of 1 jaar met toestemming)	AVG
Personeelsdossier	Tot 2 jaar na uitdiensttreding (loonbelastingdeel 7 jaar)	Arbeidswetgeving
Opleidings- en kwaliteitsregistraties	5 jaar	Arbowet
Communicatie- /contactgegevens	Zolang noodzakelijk voor communicatie	AVG
Loggingsgegevens	Maximaal 2 jaar	NEN

3.6 Nauwkeurigheid en actualiteit

De organisatie draagt zorg voor nauwkeurige en actuele gegevens. Cliënten en medewerkers zijn zelf verantwoordelijk actuele gegevens (zoals adres, contactpersoon of medische status) door te geven. Foutieve of verouderde gegevens worden zo spoedig mogelijk aangepast of verwijderd.

3.7 Pseudonimisering en anonimisering

Waar mogelijk worden persoonsgegevens gepseudonimiseerd of geanonimiseerd, met name bij:

- Interne rapportages en kwaliteitsanalyses
- Onderzoek of opleiding
- Externe rapportages aan ketenpartners of toezichthouders.

Deze maatregelen beperken de privacyrisico's en voldoen aan de principes van privacy by design en privacy by default (Bron: AVG).

4 Doeleinden van de gegevensverwerking

4.1 Algemeen uitgangspunt

Kennemerhart verwerkt persoonsgegevens uitsluitend voor vooraf vastgestelde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden hangen rechtstreeks samen met het leveren van kwalitatief goede zorg, het nakomen van wettelijke verplichtingen en het uitvoeren van interne bedrijfsprocessen.

Alle verwerkingen vinden plaats conform beginselen van doelbinding en minimale gegevensverwerking zoals opgenomen de AVG.

Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de oorspronkelijke doeleinden, tenzij daarvoor een nieuwe wettelijke grondslag of geldige toestemming bestaat.

4.2 Primaire doeleinden: Zorgverlening

Voor het uitvoeren van onze primaire taak zorgverlenen verwerken wij persoonsgegevens van zowel zorgontvangers als zorgverleners. Onder deze primaire doeleinden vallen onder andere onderstaande zaken:

Uitvoering van de behandel- of zorgovereenkomst

- Vastleggen van medische en persoonlijke gegevens die noodzakelijk zijn voor diagnostiek, behandeling, verzorging, verpleging of begeleiding (Bron: BW)
- Registratie van observaties, rapportages, medicatiegegevens, behandelplannen en zorgleefplannen.
- Communicatie met de cliënt, familie of vertegenwoordiger over de zorgverlening.

Dossiervorming en continuïteit van zorg

- Beheer van actualisatie van het zorgdossier of elektronisch cliëntendossier (ECD)
- Overdracht van gegevens aan andere zorgverleners of instellingen, wanneer dit noodzakelijk is voor een goede zorgverlening (Bron: AVG & WGBO)

Afstemming met ketenpartners

- Uitwisseling van noodzakelijke gegevens met huisartsen, apotheken, ziekenhuizen, paramedici, wijkverpleegkundigen en andere zorgverleners, binnen de wettelijke kaders van de Wabvpz en de Wegiz.

Beheer van toestemming en vertegenwoordiging:

- Vastlegging van toestemming voor zorg, gegevensuitwisseling of deelname aan onderzoek.
- Registratie van wettelijke vertegenwoordigers.

Medewerkers, vrijwilligers en stagiaires:

Voor de verwerking van persoonsgegevens van medewerkers, vrijwilligers en stagiaires gelden andere (niet-medische) grondslagen.

- Uitvoering van de arbeidsovereenkomst.
- Naleving van wettelijke verplichting (bijv. loonadministratie, pensioen, Arbowetgeving).
- Gerechtvaardigd belang van de organisatie (zoals personeelsplanning of beveiliging).

4.3 Secundaire doeleinden: Organisatie en kwaliteit van zorg

Naast het primaire doel van zorgverlening worden persoonsgegevens in beperkte mate ook gebruikt voor andere gerechtvaardigde doelen die bijdragen aan een goede bedrijfsvoering en kwaliteitsborging, waaronder:

Kwaliteitsbewaking en interne controle

- Uitvoeren van interne audits, veiligheids- en kwaliteitsonderzoeken, cliënttevredenheidsmetingen en incidentanalyses (Wkkgz)

Opleiding en training

- Gebruik van (geanonimiseerde of gepseudonimiseerde) gegevens voor opleiding- of trainingsdoeleinden binnen de organisatie, onder strikte vertrouwelijkheid.

Wetenschappelijk en statistisch onderzoek

- Alleen indien dit verenigbaar is met het doel van de oorspronkelijke gegevensverwerking en voldoet aan de voorwaarden van de AVG en de Wabvpz (bij voorkeur in geanonimiseerde vorm of met expliciete toestemming van de cliënt).

Financiële en administratieve doeleinden

- Declaraties en verantwoording aan zorgverzekeraars of zorgkantoren.
- Naleving van fiscale, boekhoudkundige en subsidieregelingen.

Beleid, planning en managementinformatie

- Opstellen van rapportages en analyses voor bedrijfsvoering, kwaliteitsverbetering en capaciteitsplanning. Hierbij worden gegevens zo veel mogelijk geanonimiseerd of geaggregeerd gebruikt.

4.4. Beveiliging, incidentenbeheer en toezicht

Voor het naleven van beveiligings- en verantwoordingsverplichtingen (Bron: AVG) worden persoonsgegevens verwerkt voor:

- Logregistraties en toegangsbeheer (wie welke gegevens heeft ingezien).
- Onderzoek en melding van datalekken of beveiligingsincidenten.
- Toezicht door de Functionaris Gegevensbescherming en interne audits.

4.5 Gebruik voor andere doeleinden

Wanneer persoonsgegevens voor een ander doel worden gebruikt dan waarvoor ze oorspronkelijk zijn verzameld, beoordeelt Kennemerhart eerst:

- Of het nieuwe doel verenigbaar is met het oorspronkelijke doel (Bron: AVG).
- Of er een nieuwe wettelijke grondslag of toestemming nodig is.
- Of de betrokkene hierover op duidelijke wijze wordt geïnformeerd.

Zonder geldige grondslag of toestemming worden persoonsgegevens niet voor andere doeleinden verwerkt.

5 Grondslagen van de verwerking

5.1 Algemeen uitgangspunt

Volgens de AVG mag Kennemerhart persoonsgegevens alleen verwerken als daarvoor een rechtmatige grondslag bestaat en, bij gezondheidsgegevens, een toegestane uitzondering (Bron: AVG).

De organisatie verwerkt geen persoonsgegevens zonder wettelijke basis, geldige overeenkomst of duidelijke toestemming. Elke verwerking wordt vooraf getoetst aan deze grondslagen en vastgesteld in het verwerkingsregister (Bron: AVG).

5.2 Grondslagen op grond van de AVG

Binnen de ouderenzorg zijn de volgende grondslagen van toepassing (bron AVG):

Uitvoering van een overeenkomst

De verwerking is noodzakelijk voor de uitvoering van een zorg- of behandelovereenkomst die met de cliënt is gesloten of een arbeidsovereenkomst die met een medewerker is gesloten. Deze grondslag geldt voor bijna alle verwerkingen die direct verband houden met de zorglening.

Wettelijke verplichting

Sommige gegevens worden verwerkt omdat de wet dit verplicht stelt. Deze grondslag geldt zonder dat toestemming van de betrokkene nodig is.

Toestemming van betrokkene

In sommige gevallen vraagt Kennemerhart expliciete toestemming voor het verwerken van persoonsgegevens, bijvoorbeeld als de verwerking niet direct voortvloeit uit de zorgverlening of een wettelijke plicht. Dit heeft een aantal voorwaarden:

- De toestemming moet vrij, specifiek, geïnformeerd en ondubbelzinnig zijn.
- De betrokkene kan de toestemming op elk moment intrekken.
- Voor cliënten jonger dan 16 jaar is toestemming van ouder voogd vereist.

Vitale belangen van betrokkene

Persoonsgegevens mogen worden verwerkt als dat noodzakelijk is om vitale belangen van de cliënt te beschermen, bijvoorbeeld bij een levensbedreigende situatie waarin toestemming niet kan worden gevraagd. Deze grondslag geldt uitsluitend bij noodsituaties waarin snel handelen vereist is.

Taak van algemeen belang of uitvoering van openbaar gezag

Zorginstellingen die publieke taken uitvoeren, kunnen persoonsgegevens verwerken als dit nodig is voor het vervullen van die taak zoals op grond van de Wet publieke gezondheid (Wpg)

Gerechtvaardigd belang

Deze grondslag geldt alleen als de verwerking noodzakelijk is voor een gerechtvaardigd belang van de organisatie of een derde, mits de belangen of fundamentele rechten van de betrokkene niet zwaarder wegen. Deze grondslag mag niet worden gebruikt voor het verwerken van gezondheidsgegevens (Zie 5.3).

5.3 Verwerking van bijzondere persoonsgegevens (gezondheidsgegevens)

De AVG verbiedt in principe de verwerking van bijzondere persoonsgegevens (zoals medische gegevens), tenzij een van de uitzonderingen uit de AVG van toepassing is. In de ouderenzorg gelden vooral de volgende uitzonderingen (bron AVG):

Medische behandeling of zorgverlening

Verwerking is toegestaan wanneer dit noodzakelijk is voor het verstrekken van gezondheidszorg of behandeling aan de cliënt, en wordt uitgevoerd door of onder verantwoordelijkheid van een zorgprofessional met geheimhoudingsplicht (zoals vastgelegd in de WGBO en de Wet BIG).

Volksgezondheid en zorgveiligheid

Verwerking is toegestaan voor doeleinden op het gebied van volksgezondheid, zoals het waarborgen van hoge normen van kwaliteit en veiligheid in de zorg.

Toestemming van betrokkene

Indien geen andere uitzondering van toepassing is, kan verwerking plaatsvinden met uitdrukkelijke toestemming van de cliënt.

Archivering en wetenschappelijk onderzoek

Verwerking is toegestaan voor historische, statistische of wetenschappelijke doeleinden, mits passende waarborgen zijn getroffen, zoals pseudonimisering of anonimisatie van gegevens.

5.4 Verhouding tot de WGBO en Wabvpz

Naast de AVG gelden binnen de ouderenzorg specifieke regels uit de WGBO en de Wabvpz:

- WGBO verplicht de zorgverlener tot het bijhouden van een zorgdossier en het bewaren daarvan gedurende 20 jaar.
- Wabvpz regelt de elektronische verwerking, inzage en logging van gegevens in zorgsystemen.
- Beide wetten ondersteunen de grondslagen van de AVG en verduidelijken hoe deze in de zorgpraktijk moet worden toegepast.

5.5 Documentatieplicht en verantwoording

Kennemerhart houdt een verwerkingsregister bij conform de AVG, waarin voor elke categorie van verwerkingen is vastgelegd:

- Het doel van de verwerking
- De wettelijke grondslag
- De categorieën van persoonsgegevens en betrokkenen
- De bewaartermijnen
- De beveiligingsmaatregelen
- Eventuele ontvangers of verwerkers

Dit register vormt het bewijs van naleving van de verantwoordingsplicht

6 Beveiliging van persoonsgegevens

6.1 Algemeen uitgangspunt

Kennemerhart treft passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies, ongeoorloofde toegang, wijziging of openbaarmaking (Bron: AVG).

De beveiliging is afgestemd op:

- De aard en gevoeligheid van de gegevens (met name medische gegevens).
- De risico's voor de rechten en vrijheden van betrokkenen.
- De stand van de techniek en de kosten van uitvoering
- De vereisten uit de NEN-normen voor informatiebeveiliging in de zorg.

De organisatie hanteert het principe van "privacy by design en privacy by default": Persoonsgegevens worden zo ontworpen, ingericht en beheerd dat privacy standaard wordt gewaarborgd.

6.2 Beveiligingsbeleid en verantwoordelijkheden

Beveiligingsbeleid

De organisatie heeft een vastgesteld en actueel informatiebeveiligingsbeleid, dat minimaal tweejaarlijks wordt herzien en goedgekeurd door het bestuur.

Het beleid beschrijft onder andere:

- Beveiligingsdoelen en uitgangspunten
- Rollen en verantwoordelijkheden
- Classificatie van informatie
- Incidentenreglement
- Continuïteits- en herstelprocedures.

Binnen Kennemerhart zijn verschillende functionarissen verantwoordelijk voor privacy en informatiebeveiliging. Zij werken nauw samen binnen één geïntegreerd kader van gegevensbescherming en cybersecurity:

Bestuur

Draagt eindverantwoordelijkheid voor naleving van de AVG, NIS2 en informatiebeveiligingsnormen. Het bestuur stelt beleid vast, faciliteert middelen en ziet toe op de uitvoering.

Functionaris Gegevensbescherming (FG)

Houdt onafhankelijk toezicht op naleving van de AVG, adviseert over privacyrisico's, beoordeelt DPIA's en is aanspreekpunt voor betrokkenen en de Autoriteit Persoonsgegevens.

Chief Information Security Officer (CISO)

Verantwoordelijk voor het strategische informatiebeveiligingsbeleid, risicomanagement, NIS2-naleving en coördinatie van beveiligingsincidenten. De CISO bewaakt de samenhang tussen IT, zorgsystemen en privacy.

Security Officer (SO)

Een Security Officer is verantwoordelijk voor het bewaken, implementeren en verbeteren van het informatiebeveiligingsbeleid binnen een organisatie. De rol richt zich op het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

Risico- en procescontroller (RPC)

De FG, CISO en RPC overleggen periodiek met elkaar en rapporteren gezamenlijk aan het bestuur over privacy, beveiliging en compliance. Deze samenwerking waarborgt een geïntegreerde aanpak van gegevensbescherming, ethiek en digitale veiligheid.

6.3 Technische beveiligingsmaatregelen

Kennemerhart technische maatregelen toe, conform de NEN en AVG, beschreven in het informatiebeveiligingsbeleid die periodiek wordt gecontroleerd.

Kennemerhart voldoet aan de eisen uit de Europese NIS2-richtlijn, waarin aanvullende verplichtingen gelden voor netwerk- en informatiebeveiliging. Deze verplichtingen betreffen risicobeheer, continuïteit van dienstverlening, en meldingen van ernstige cyberincidenten aan de bevoegde autoriteiten. De organisatie houdt hierbij rekening met de samenloop tussen NIS2 en de AVG.

6.4 Datalekken en incidentenmanagement

Kennemerhart heeft een procedure voor het melden en afhandelen van datalekken conform de AVG van de richtlijnen van de Autoriteit Persoonsgegevens. De wijze van afhandelen van datalekken is overzichtelijk en bereikbaar voor het personeel van de organisatie.

7 Digitale Zorgtoepassingen

7.1 Algemeen uitgangspunt

Kennemerhart zet digitale technologieën in om de kwaliteit, veiligheid en efficiëntie van zorg te verbeteren. Deze toepassingen worden uitsluitend gebruikt als zij bijdragen aan mensgerichte zorg en het welzijn van cliënten, met behoud van privacy en autonomie.

7.2 Technologieën in gebruik

Binnen de ouderenzorg worden onder meer de volgende digitale hulpmiddelen toegepast:

- Sensortechnologie: Valdetectie, bewegingssensoren en slimme bedmatten om risico's tijdig te signaleren.
- Camera's: Beperkt en uitsluitend in gemeenschappelijke ruimtes voor veiligheid en incidentregistratie.
- Wearables: Apparaten die vitale functies meten (hartslag, activiteit) en waarschuwen bij afwijkingen.
- Domotica: Slimme verlichting, automatische deuropeners en spraakgestuurde assistenten ter ondersteuning van zelfredzaamheid.

7.3 Voorwaarden voor gebruik

Het gebruik van deze technologieën vindt plaats onder strikte voorwaarden:

- Risico-inventarisatie: Voorafgaande aan het gebruik van een nieuw digitaal hulpmiddel (DPIA)
- Toestemming: Cliënten worden vooraf geïnformeerd en geven expliciete toestemming voor inzet van sensoren, wearables of cameratoezicht (Bron: AVG)
- Proportionaliteit: De inzet is beperkt tot wat noodzakelijk is voor veiligheid en zorgcontinuïteit. Alternatieven zonder privacy-impact worden altijd eerst overwogen.
- Transparantie: Cliënten en familie worden duidelijk geïnformeerd over doel, werking en bewaartermijnen van gegevens.

7.4 Waarborging van privacy en autonomie

Kennemerhart hanteert het principe van privacy by design en privacy by default:

- Gegevens worden zo veel mogelijk lokaal verwerkt en niet gedeeld met derden zonder grondslag.
- Camerabeelden worden maximaal 4 weken bewaard, tenzij een incident onderzoek vereist.
- Sensordata en wearable-informatie worden alleen gekoppeld aan het zorgdossier indien relevant voor behandeling.
- Cliënten behouden zo veel mogelijk regie: technologie kan op verzoek worden uitgeschakeld, tenzij vitale belangen in het geding zijn.

8 Delen van persoonsgegevens met derden

8.1 Algemeen uitgangspunt

Kennemerhart gaat zorgvuldig om met het delen van persoonsgegevens met derden. Gegevens worden uitsluitend gedeeld:

- Als dat noodzakelijk is voor de uitvoering van de zorgverlening.
- Als de betrokkene daarvoor toestemming heeft gegeven.
- Als dit verplicht is op grond van wet- en regelgeving.

Het uitgangspunt is altijd: niet meer gegevens delen dan strikt noodzakelijk

8.2 Wettelijke grondslagen voor gegevensdeling

Volgens de AVG en zorgspecifieke wetten mag persoonsgegevensverwerking alleen plaatsvinden op basis van één van de volgende grondslagen:

Toestemming van de betrokkene

- De betrokkene heeft uitdrukkelijk toestemming gegeven voor het delen van gegevens.
- Toestemming moet vrij, specifiek, geïnformeerd en ondubbelzinnig zijn.
- De betrokkene kan deze toestemming te allen tijde intrekken.

Uitvoering van de behandelovereenkomst (WGBO)

- Voor goede zorgverlening is het noodzakelijk dat gegevens worden gedeeld met zorgprofessionals die direct bij de behandeling betrokken zijn.

Wettelijke verplichting

- Gegevens moeten worden gedeeld op basis van specifieke wettelijke plicht, zoals meldingen aan het CIZ, RIVM, Inspectie Gezondheidszorg en Jeugd (IGJ) op grond van de Wkkgz of Wvvgz.

Vitaal belang voor betrokkene

- In noodsituaties waarin de cliënt niet in staat is toestemming te geven mogen noodzakelijke gegevens worden gedeeld voor levensreddende zorg.

Gerechtvaardigd belang

- In beperkte gevallen, bijvoorbeeld bij cameratoezicht of fraudepreventie, mits de privacybelangen van betrokkenen niet zwaarder wegen.

8.3 Delen van gegevens binnen de zorgketen

Behandelteam in interne overdracht

- Binnen Kennemerhart worden cliëntgegevens gedeeld tussen medewerkers die direct betrokken zijn bij de zorgverlening.
- Deze gegevensverdeling is noodzakelijk voor continuïteit van kwaliteit van zorg.
- Elk teamlid heeft een geheimhoudingsplicht.

Overdracht naar andere zorgaanbieders

- Bij doorverwijzing of ontslag worden relevante gegevens overgedragen aan de volgende zorgverlener.
- Dit gebeurt alleen met toestemming van de cliënt, tenzij de overdracht noodzakelijk is voor diens zorgcontinuïteit.

8.4 Delen van gegevens met mantelzorgers en familie

In de ouderzorg speelt communicatie met familie en mantelzorgers een grote rol. Toch geldt ook hier: de cliënt bepaalt.

Wilsbekwame cliënt

- Alleen met toestemming van de cliënt mogen gegevens worden gedeeld met familie of mantelzorgers.
- Toestemming kan mondeling of schriftelijk worden vastgelegd in het zorgdossier.

Wilsonbekwame cliënt

- In dat geval treedt de wettelijke vertegenwoordiger op namens de cliënt.
- Familieleden die niet formeel vertegenwoordiger zijn, krijgen alleen algemene informatie en geen medische details.

Overlijden van de cliënt

- Na overlijden geldt het medisch beroepsgeheim nog steeds.
- Gegevens mogen alleen worden verstrekt als de cliënt bij leven toestemming gaf, of als zwaarwegende belangen dit rechtvaardigen.

8.5 Delen van gegevens met externe partijen (verwerkers en derden)

Kennemerhart werkt samen met verschillende externe partijen die persoonsgegevens verwerken, zoals ICT-leveranciers, laboratoria, arbodiensten en salarisverwerkers.

Verwerkers

- Een verwerker is een partij die in opdracht van Kennemerhart gegevens verwerkt.
- Met alle verwerkers wordt een verwerkersovereenkomst gesloten conform de AVG. Deze bevat bepalingen over:
 - o Beveiligingsmaatregelen (NEN-niveau)
 - o Geheimhouding en auditrechten
 - o Datalekmeldingen en subverwerkers
 - o Verwijdering van gegevens na afloop van de overeenkomst

Derden

- Soms worden gegevens gedeeld met partijen die zelf verwerkingsverantwoordelijke zijn, zoals:
 - o Huisartsen of specialisten
 - o Zorgverzekeraars
 - o Inspecties of toezichthouders
- In die gevallen blijft elke partij zelf verantwoordelijk voor de rechtmatige verwerking van de ontvangen gegevens.

8.6 Wettelijk meld- en rapportageverplichtingen

Kennemerhart is wettelijk verplicht om bepaalde gegevens te verstrekken aan overheidsinstanties of toezichthouders, bijvoorbeeld:

- IGJ
- AP
- RIVM
- CIZ of gemeente
- Zorgverzekeraars

In al deze gevallen worden alleen de noodzakelijke gegevens verstrekt, en indien mogelijk geanonimiseerd.

8.7 Gegevensdeling in elektronische zorgsystemen

Elektronische gegevensuitwisseling

- Gegevensuitwisseling met andere zorgaanbieders gebeurt uitsluitend via beveiligde systemen die voldoen aan de NEN-normen
- Alleen geautoriseerde zorgverleners hebben toegang via beveiligde platforms.

Toestemming voor elektronische uitwisseling

- De cliënt moet actieve toestemming geven voordat medische gegevens elektronisch worden gedeeld buiten de organisatie.
- De toestemming wordt vastgelegd in het elektronisch dossier en kan te allen tijde worden ingetrokken.

8.8 Delen van gegevens met toezichthouders, politie of justitie.

In sommige situaties is de organisatie verplicht of bevoegd gegevens te delen met overheidsinstanties:

- Politie of justitie: Alleen bij geldig bevel of wettelijke grondslag.
- AP: Bij toezicht op naleving van privacywetgeving.
- IGJ: Bij onderzoeken of calamiteiten in het kader van de Wkkgz.

In alle gevallen wordt vooraf getoetst of de gevraagde gegevens noodzakelijk en proportioneel zijn.

8.9 Geanonimiseerde of gepseudonimiseerde gegevens

Voor onderzoek, kwaliteitsverbetering en beleid kan Kennemerhart gebruikmaken van geanonimiseerde gepseudonimiseerde gegevens:

- Geanonimiseerde gegevens bevatten geen identificeerbare informatie meer en vallen niet onder de AVG.
- Gepseudonimiseerde gegevens kunnen nog worden herleid via een code en vallen wel onder de AVG, zolang de sleutel bestaat.
- Bij gebruik voor onderzoek of statistiek wordt voldaan aan de Wet medisch-wetenschappelijk onderzoek met mensen of het kwaliteitsregistersysteem.

8.10 Transparantie over gegevensdeling

Kennemerhart informeert cliënten, medewerkers en andere betrokkenen helder over:

- Met wie hun gegevens worden gedeeld
- Op welke grondslag
- Voor welke doeleinden
- Welke beveiligingsmaatregelen worden genomen

Deze informatie is opgenomen:

- In de privacyverklaring op de website
- Het cliënteninformatieboekje

9 Rechten van betrokkenen

9.1 Algemeen uitgangspunt

Iedere natuurlijke persoon van wie Kennemerhart persoonsgegevens verwerkt (de betrokkene), heeft bepaalde rechten op grond van de AVG. Daarnaast gelden voor cliënten aanvullende rechten op basis van de WGBO en de Wabvpz.

De organisatie respecteert en faciliteert deze rechten zorgvuldig, transparant en binnen de wettelijke termijnen.

9.2 Categorieën van betrokkenen met rechten

De volgende personen kunnen hun rechten uitoefenen:

- Cliënten en/of bewoners
- Wettelijke vertegenwoordigers, mantelzorgers en contactpersonen
- Medewerkers, vrijwilligers en stagiaires
- Zorgverleners en ketenpartners
- Leveranciers en dienstverleners (verwerkers)
- Bezoekers en relaties

9.3 Overzicht van rechten onder de AVG

De AVG kent de volgende privacyrechten:

Nr.	Recht	Korte omschrijving
1	Recht op informatie	Betrokkene moet duidelijk worden geïnformeerd over het gebruik van zijn gegevens.
2	Recht op inzage	Betrokkene mag inzien welke gegevens over hem zijn vastgelegd.
3	Recht op correctie (rectificatie)	Onjuiste of onvolledige gegevens moeten worden verbeterd.
4	Recht op verwijdering (recht op vergetelheid)	Gegevens moeten worden verwijderd als ze niet langer nodig zijn of onrechtmatig worden verwerkt.
5	Recht op beperking van verwerking	Tijdelijke beperking van verwerking bij twijfel over juistheid of rechtmatigheid
6	Recht op overdraagbaarheid (dataportabiliteit)	Recht om gegevens over te dragen aan een andere organisatie
7	Recht van bezwaar	Betrokkene kan bewaar maken tegen verwerking op grond van gerechtvaardigd of algemeen belang.
8	(AI-act) Recht om niet te worden onderworpen aan geautomatiseerde besluitvorming	Geen beslissing uitsluitend op basis van automatische verwerking of AI zonder menselijke tussenkomst.

9.4 Procedure voor uitoefening van rechten

Kennemerhart heeft een vastgestelde procedure voor het indienen en afhandelen van verzoeken:

Indienen van het verzoek

- Het verzoek kan schriftelijk, per e-mail of via een speciaal formulier worden ingediend bij de FG via privacy@kennemerhart.nl
- De identiteit van de verzoeker wordt altijd geverifieerd

Behandelingstermijn

- De organisatie reageert binnen één maand na ontvangst van het verzoek.
- Deze termijn kan maximaal met twee maanden worden verlengd bij complexe verzoeken (bron: AVG)

Kosten

- Verzoeken zijn kosteloos, tenzij het gaat om herhaalde of kennelijk ongegronde verzoeken (bron: AVG)

Besluitvorming

- De FG beoordeelt of het verzoek rechtmatig is en overlegt zo nodig met de behandelend zorgverlener of HR-afdeling.
- Indien het verzoek (gedeeltelijk) wordt afgewezen, ontvangt de betrokkene een gemotiveerde toelichting.

Documentatie en logging

- Elk verzoek en afhandeling worden geregistreerd in het interne register van privacyverzoeken.

9.5 Beperkingen op grond van andere wetgeving

In uitzonderlijke gevallen kan een verzoek worden geweigerd of beperkt geweigerd, bijvoorbeeld:

- Als de gegevens noodzakelijk zijn voor een lopend onderzoek of rechtszaak.
- Als verwijdering in strijd is met wettelijke bewaarplichten.
- Als de privacy van andere betrokkenen wordt geschaad.
- Als sprake is van een gerechtvaardigd belang van de organisatie dat zwaarder weegt.

In alle gevallen worden de betrokkene schriftelijk geïnformeerd over de reden van afwijzing en het recht op klacht bij de AP.

9.6 Uitoefening van rechten door vertegenwoordigers

Wanneer een cliënt wilsonbekwaam is of niet zelf kan handelen:

- Mag de wettelijke vertegenwoordiger of mentor/curator de rechten namens hem/haar uitvoeren.
- De vertegenwoordiger moet aantonen dat hij daartoe bevoegd is.
- Bij twijfel over de bekwaamheid wordt overleg gevoerd met de behandelend zorgverlener.

9.7 Klachten en geschillen

Als een betrokkene ontevreden is over de wijze waarop zijn gegevens worden verwerkt of over de afhandeling van een verzoek, kan hij:

- Een klacht indienen bij de FG.
- Een klacht indienen bij de klachtenfunctionaris of via de reguliere klachtenprocedure.
- Een formele klacht indienen bij de AP

- Zich wenden tot de rechter als laatste middel.

Functionaris Gegevensbescherming:

Anat Fuldauer

privacy@kennemerhart.nl

Autoriteit Persoonsgegevens (AP)

Website: www.autoriteitpersoonsgegevens.nl

Telefoon: 088-1805-250

9.9 Transparantie & communicatie

Kennemerhart communiceert helder, begrijpelijk en in toegankelijke taal over privacyrechten passend bij de doelgroep van de ouderenzorg. Waar nodig ondersteunt de organisatie cliënten en familieleden bij het indienen van verzoeken via hulp van cliëntondersteuners, uitleg en ondersteuning door zorgmedewerkers.

10 Kunstmatige Intelligentie (AI)

10.1 Algemeen uitgangspunt

Kennemerhart gebruikt in toenemende mate digitale hulpmiddelen die (deels) worden aangestuurd door kunstmatige intelligentie (AI). Dit kan variëren van toepassingen die zorgprocessen ondersteunen, zoals valdetectie of medicatiebewaking, tot systemen die administratieve taken of dataverwerking verbeteren.

Het uitgangspunt blijft dat AI alleen wordt ingezet als dit bijdraagt aan veilige, verantwoorde en mensgerichte zorg, met behoud van regie voor cliënten en medewerkers. AI wordt nooit gebruikt om zonder menselijke tussenkomst besluiten te nemen die invloed hebben op de zorg of het welzijn van cliënten.

10.2 Transparantie en menselijke controle

Kennemerhart zorgt ervoor dat bij elke AI-toepassing duidelijk is:

- Welke gegevens worden gebruikt.
- Met welk doel.
- Welke keuzes het systeem ondersteunt of automatiseert.
- Welke persoon verantwoordelijk blijft voor de uiteindelijke beslissing.

Er blijft altijd sprake van menselijke controle. Zorgprofessionals behouden de verantwoordelijkheid om AI-adviezen te beoordelen en in context te plaatsen.

10.3 Gegevensverwerking en privacy

AI-systemen kunnen persoonsgegevens verwerken, waaronder mogelijk gezondheidsgegevens. Dit gebeurt uitsluitend:

- Op basis van een rechtmatige grondslag (Bron: AVG)
- Met dataminimalisatie en pseudonimisering waar mogelijk.
- Binnen beveiligde omgevingen die voldoen aan de NEN-normen.
- Alleen met betrouwbare leveranciers waarmee een verwerkingsovereenkomst is afgesloten.

Kennemerhart voert een Fundamental Rights Impact Assessment (FRIA) uit bij AI-toepassingen met een verhoogd risico voor privacy of autonomie van betrokkene.

10.4 Ethisch kader en zorgvuldigheid

Naast naleving van wetgeving worden AI-toepassingen beoordeeld op ethische waarden die binnen de ouderenzorg en Kennemerhart centraal staan. Kennemerhart volgt bij dit alles de principes van transparantie, uitlegbaarheid en verantwoord gebruik van AI zoals vastgelegd in de EU AI Act en richtlijnen van de AP.

10.5 Toezicht en evaluatie

Nieuwe AI-toepassingen worden periodiek geëvalueerd op:

- Effectiviteit en betrouwbaarheid
- Naleving van AVG- en ethische normen
- Meldingen of incidenten in het gebruik

Eventuele aanpassingen of risico's worden vastgelegd in het privacyregister en besproken met het bestuur en betrokken afdelingen.

11 Gebruik van data-analyse en big data

11.1 Doel en uitgangspunten

Kennemerhart gebruikt data-analyse uitsluitend voor kwaliteitsverbetering, beleidsontwikkeling en wetenschappelijk onderzoek. Dit gebeurt:

- Met geanonimiseerde of gepseudonimiseerde gegevens, conform de AVG
- Binnen beveiligde omgevingen die voldoen aan de NEN-normen
- Onder toezicht van een ethische commissie bij onderzoek met impact op cliënten.

11.2 Waarborgen

- Geen herleidbare persoonsgegevens worden gebruikt voor analyses.
- Voor nieuwe projecten met verhoogd privacyrisico wordt een Data Protection Impact Assessment (DPIA) uitgevoerd.
- Transparantie: cliënten worden geïnformeerd via de privacyverklaring en kunnen bezwaar maken tegen gebruik van hun gegevens voor secundaire doeleinden.

Bijlage: Toelichting Bij Privacyreglement: Stand van zaken

Kennemerhart en privacybescherming

Kennemerhart hecht grote waarde aan de bescherming van persoonsgegevens van cliënten, medewerkers en samenwerkingspartners. Het privacyreglement beschrijft de verplichtingen die voortvloeien uit relevante wet- en regelgeving en vormt het kader voor een zorgvuldige en transparante omgang met persoonsgegevens. Privacybescherming heeft bij Kennemerhart een vaste en belangrijke plaats binnen de organisatie.

Kennemerhart werkt continu aan het verder versterken van privacybescherming en informatiebeveiliging. Doorlopend worden processen, maatregelen en kennis verder ontwikkeld en geprofessionaliseerd, zodat deze blijven aansluiten bij actuele wetgeving en maatschappelijke verwachtingen. Hiermee borgt Kennemerhart dat zorgvuldig omgaan met persoonsgegevens een integraal en toekomstbestendig onderdeel is van de organisatie.